

## PATENT COOPERATION TREATY



PCT

NOTIFICATION OF RECEIPT OF  
RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

HARADA, Kazuo  
Nishizawa Bldg. 5th Floor  
18-8, Minamisaiwai 2-chome, Nishi-  
ku  
Yokohama-shi, Kanagawa 220-0005  
JAPON

Date of mailing (day/month/year) 26 July 2001 (26.07.01)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 0151268	International application No. PCT/JP01/05525

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

FUJITSU LIMITED (for all designated States except US)  
MAKITA, Ikuo et al (for US)

International filing date : 27 June 2001 (27.06.01)  
Priority date(s) claimed :  
Date of receipt of the record copy  
by the International Bureau : 13 July 2001 (13.07.01)  
List of designated Offices :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR  
National : AU, CA, CN, ID, JP, KR, MX, SG, US, VN

## ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase  
☒ confirmation of precautionary designations  
☐ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer:  Shinji IGARASHI
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

**INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE**

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

**CONFIRMATION OF PRECAUTIONARY DESIGNATIONS**

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

**REQUIREMENTS REGARDING PRIORITY DOCUMENTS**

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2003年1月9日 (09.01.2003)

PCT

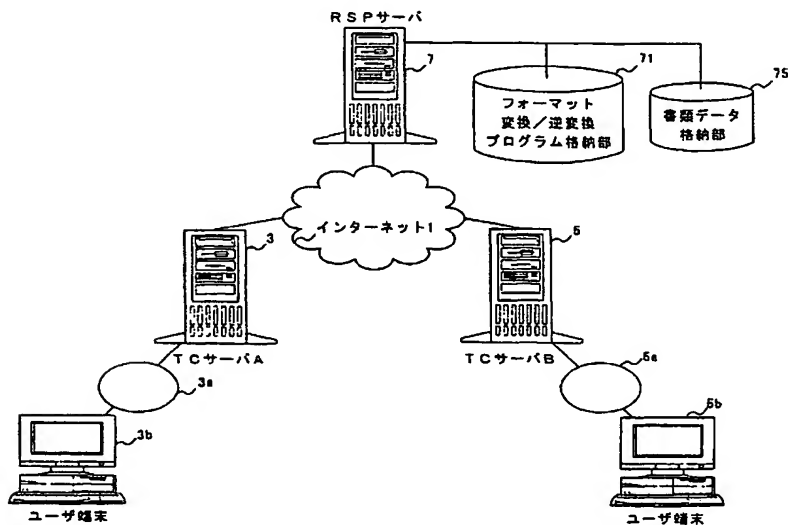
(10) 国際公開番号  
WO 03/003329 A1

- (51) 国際特許分類<sup>7</sup>: G09C 1/00 (72) 発明者; および  
(75) 発明者/出願人 (米国についてのみ): 蒔田育生 (MAKITA, Ikuo) [JP/JP]. 石川利久 (ISHIKAWA, Toshihisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP01/05525
- (22) 国際出願日: 2001年6月27日 (27.06.2001)
- (25) 国際出願の言語: 日本語 (74) 代理人: 原田一男 (HARADA, Kazuo); 〒220-0005 神奈川県横浜市西区南幸二丁目18番8号 西沢ビル5階 Kanagawa (JP).
- (26) 国際公開の言語: 日本語
- (81) 指定国 (国内): AU, CA, CN, ID, JP, KR, MX, SG, US, VN.
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[続葉有]

(54) Title: DATA ORIGINALITY VALIDATING METHOD AND SYSTEM

(54) 発明の名称: データのオリジナリティ検証方法及びシステム



(57) Abstract: A PSC server (7) receives a first set of data and a first electronic signature for the first set of data from a TC server (3), converts the format of the received first set of data to the one corresponding to the destination to which the first set of data is sent thereby to create a second set of data, and sends at least the second set of data, a format reverse-conversion program for reverse-conversion of the format, and the first electronic signature to a TC server (5) concerning the transmission destination. By thus sending the format reverse-conversion program and the first electronic signature, it is possible for the TC server (5) to confirm that the first set of data is not altered falsely, namely confirmation of the TC server (3), or the transmission source, can be attained.

- 3b...USER TERMINAL  
3...TC SERVER A  
1...INTERNET  
7...RSP SERVER  
71...FORMAT CONVERSION/REVERSE-CONVERSION PROGRAM STORAGE UNIT  
75...DOCUMENT DATA STORAGE UNIT  
5...TC SERVER B  
5b...USER TERMINAL

[続葉有]

WO 03/003329 A1



添付公開書類:  
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

RSPサーバ7は、TCサーバ3から第1のデータと少なくとも当該第1のデータに対する第1の電子署名とを受信する。次に、受信された第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成する。そして、少なくともフォーマット変換において生成された第2のデータとフォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと第1の電子署名とを送信先に関連するTCサーバ5に送信する。このようにフォーマット逆変換プログラムとフォーマット変換前の第1のデータに対する第1の電子署名とを送信することにより、TCサーバ5において第1のデータが改竄等されていないことを確認することができるようになる。すなわち、送信元であるTCサーバ3の確証を得ることができるようになる。

- 1 -

## 明細書

## データのオリジナリティ検証方法及びシステム

## 5    [技術分野]

本発明は、データ通信技術に関し、より詳しくはデータのオリジナリティ検証技術に関する。

## [背景技術]

- 10    電子商取引においては、取引を行う契約書等の書類データが改竄されないように、書類データに対して所定のハッシュアルゴリズムが適用され、生成されたハッシュ値は暗号化され電子署名が生成される。そして、暗号化された書類データと共に電子署名を取引相手に送信する。取引相手は、書類データを復号化し、さらに所定のハッシュアルゴリズムを適用してハッシュ値を生成する。また、電子署名も復号化してハッシュ値を復元し、生成されたハッシュ値と比較することにより、改竄等が行われていないことを確認することができる。このような技術を用いれば二社間の取引であれば問題なく処理できる。
- 15

- しかし、国際貿易業務においては、多数の会社や各種行政機関等が関連している。このような会社や行政機関同士の二社間の通信においては上で述べたような技術
- 20    技術を適用すればよいが、三社以上の会社や行政機関等が関わる書類データが通信される場合には必ずしも上で述べたような技術では十分ではない。例えばAからBを経由してCに書類データを送信する場合に、Aにおいて生成された書類データが、Cのシステムや法制上そのままの形式では処理できない場合が生ずる。この際Bが書類データにCのシステムや法制等に合わせてフォーマット変換を
- 25    施す場合があるが、このようなフォーマット変換を施すと送信元たるAの確証は得られなくなってしまう。

## [発明の開示]

よって本発明の目的は、書類データが途中で変更される場合であっても送信元

の確証を得られるようにするための技術を提供することである。

上記目的を達成するために、本発明の第1の態様に係る例えばR S P (Repository Service Provider) サーバにより実施される情報処理方法は、第1のコンピュータ (例えばT C (Trade Chain) サーバ) から第1のデータ (例えばインボイス等の書類データ) と少なくとも当該第1のデータに対する第1の電子署名とを受信する受信ステップと、受信ステップにおいて受信された第1のデータに対して当該第1のデータの送信先 (例えば直接の送信先だけでなく、国名などの場合を含む) に対応するフォーマット変換を実施し、第2のデータを生成するフォーマット変換ステップと、少なくともフォーマット変換ステップにおいて生成された第2のデータとフォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと第1の電子署名とを送信先に関連する第2のコンピュータ (例えば送信先のT Cサーバ) に送信する送信ステップとを含む。

このようにフォーマット逆変換プログラムとフォーマット変換前の第1のデータに対する第1の電子署名とを送信することにより、第2のコンピュータにおいて第1のデータが改竄等されていないことを確認することができるようになる。すなわち、送信元である第1のコンピュータ又はその管理・運営者の確証を得ることができるようになる。

なお、上で述べた受信ステップにおいて、少なくともフォーマット逆変換プログラムに対する第3の電子署名をさらに受信するような場合もある。第1のコンピュータにおいてフォーマット逆変換プログラムを送信先に対して保証するような場合もある。なお、フォーマット逆変換プログラムをさらに受信する場合もある。

25

さらに、第1のコンピュータから送信先の指定を含むフォーマット逆変換プログラムの送信要求を受信するステップと、送信先に対応するフォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、第1のコンピュータに送信するステップとをさらに含む場合もある。このようにして送信した

フォーマット逆変換プログラムに対する電子署名が第1のコンピュータにて生成される。

- 本発明の第2の態様に係る例えばRSPサーバにより実施される情報処理方法
- 5 法は、第1のコンピュータから第1のデータと少なくとも当該第1のデータに対する第1の電子署名とを受信する受信ステップと、受信ステップにおいて受信された第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成するフォーマット変換ステップと、少なくともフォーマット変換ステップにおいて生成された第2のデータとフォーマット
- 10 変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報（例えばフォーマット逆変換プログラムのID又は送信元である第1のコンピュータの情報によりフォーマット逆変換プログラムを特定できる場合には送信元の情報）と第1の電子署名とを送信先に関連する第2のコンピュータに送信する送信ステップとを含む。
- 15 例えば第2のコンピュータにフォーマット逆変換プログラムが保持されている場合には、フォーマット逆変換プログラムを送信せずともその識別情報を送信するだけで、第2のコンピュータにおいて、第2のデータをフォーマット逆変換し、第1のデータを復元することができるようになる。
- 20 本発明の第3の態様に係る例えば送信元のTCサーバにより実施される情報処理方法は、データのフォーマット変換を実施するコンピュータ（例えば実施例のRSPサーバ）に対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、データのフォーマット変換を実施するコンピュータからフォーマット逆
- 25 変換プログラムを受信した場合には、少なくともフォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された電子署名とデータと当該データに対する電子署名とを上記データのフォーマット変換を実施するコンピュータに送信する送信ステップとを含む。なお、フォーマット逆変換プログラムをデータのフォーマット変換を実施するコンピュータにさらに送信する場合もある。

このようにすることにより送信先のコンピュータ（例えば送信先のTCサーバ）に送信されたフォーマット逆変換プログラムの改竄の有無などを確認することができるようになる。

- 5      本発明の第4の態様に係る例えば送信元のTCサーバにおいて実施される情報処理方法は、データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、データのフォーマット変換を実施するコンピュータからフォーマット逆変換プログラムを受信した場合
- 10      には、少なくともフォーマット逆変換プログラム及びデータに対する電子署名を生成し、少なくとも生成された電子署名とデータとをデータのフォーマット変換を実施するコンピュータに送信する送信ステップとを含む。本発明の第3の態様とは異なる形で電子署名を生成して送信する場合もある。

- 15      本発明の第5の態様に係る例えば送信先のTCサーバにおいて実施される情報処理方法は、送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、受信されたフォーマット逆変換プログラムを用いて上記フォーマット変換されたデータ
- 20      を逆変換し、逆変換データを生成するステップと、少なくとも逆変換データから第1ハッシュ値を計算するステップと、受信された電子署名から第2ハッシュ値を復元するステップと、計算された第1ハッシュ値と復元された第2ハッシュ値とを比較して改竄の有無を判断するステップとを含む。

- 25      このようにすればRSPサーバ等でフォーマット変換が実施されていても、RSPサーバ等の処理の前に元のデータに対して改竄等が行われていないか等を判断することができるようになる。すなわち、送信元の確証を得ることができるようになる。

なお、上で述べた受信ステップにおいて、フォーマット逆変換プログラムに対



- する第2の電子署名を受信し、プログラム逆変換プログラムから第3ハッシュ値を計算するステップと、第2の電子署名から第4ハッシュ値を復元するステップと、計算された第3ハッシュ値と復元された第4ハッシュ値とを比較して改竄の有無を判断するステップとをさらに含む場合もある。このようにフォーマット逆変換プログラムに対する第2の電子署名を受信すれば、送信元の認証を得たフォーマット逆変換プログラムであって、改竄等が行われていないことを確認できるようになる。

- 本発明の第6の態様に係る例えば送信先のTCサーバにより実施される情報処理方法は、送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、受信されたフォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、抽出されたフォーマット逆変換プログラムを用いてフォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、逆変換データから第1ハッシュ値を計算するステップと、受信された電子署名から第2ハッシュ値を復元するステップと、計算された第1ハッシュ値と復元された第2ハッシュ値とを比較して改竄の有無を判断するステップとを含む。
- このようにフォーマット逆変換プログラムを送信先のTCサーバで保持している場合にはデータを送信する都度にフォーマット逆変換プログラムを送信せずに、当該フォーマット逆変換プログラムを識別するための識別情報を送信すればよい。但し、送信元の国などが分かればフォーマット逆変換プログラムを特定できる場合もあり、必ずしもフォーマット逆変換プログラムのIDが必要なわけではない。

なお、本発明の第1乃至第6の態様に係る情報処理方法をコンピュータに実行させるためのプログラムを作成することも可能であって、当該プログラムは、例えばフロッピー・ディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハ

ードディスク等の記憶媒体又は記憶装置に格納される。また、インターネットなどのネットワークを介して配布される場合もある。なお、処理途中のデータについては、コンピュータのメモリに一時保管される。

5     〔図面の簡単な説明〕

第1図は、実施例1のシステム概要を示す図である。

第2図は、フォーマット変換／逆変換プログラム格納部に格納された管理テーブルの一例を示す図である。

第3図は、電子署名及び暗号化方式を示す図である。

10    第4図は、実施例1の処理の概要を示す図である。

第5図は、実施例1の処理フローを示すフローチャートである。

第6図は、実施例2の処理の概要を示す図である。

第7図は、実施例2の処理フローを示すフローチャートである。

第8図は、実施例2のシステム概要を示す図である。

15    第9図は、フォーマット逆変換プログラム格納部に格納された管理テーブルの一例を示す図である。

第10図は、実施例3の処理の概要を示す図である。

第11図は、実施例3の処理フローを示すフローチャートである。

20    〔本発明を実施するための最良の形態〕

〔実施例1〕

本発明の実施例1に係るシステム概要図を第1図に示す。実施例1は、本発明を貿易EDI (Electric Data Interchange) システムに適用した場合の第一の例である。ここでは、企業Aから企業Bに書類データを送信する必要があるが、  
25    例えば企業Aの属する国の法制等に従った書類データを企業Bの属する国の法制等に従った書類データに変換しなければならない場合を想定する。

コンピュータ・ネットワークであるインターネット1には、例えばインボイス等の書類データの送信元である企業Aが管理・運用しているTCサーバA (3) と、例えば書類データのフォーマット変換や書類データの蓄積サービスなどを提

供するためのRSPサーバ7と、例えば書類データの送信先である企業Bが管理・運営しているTCサーバB(5)とが接続されている。なお、TCサーバは2つだけでなく多数インターネット1に接続されている。また、RSPサーバ7も1つだけでなく複数存在している場合もある。

- 5 TCサーバA(3)は、例えばLAN(Local Area Network)3aを介して1又は複数のユーザ端末3bに接続している。なお、LANではなく、インターネット等の他のネットワークを経由するような構成であってもよい。企業Aの社員はユーザ端末3bを操作して、書類データの送信などをTCサーバA(3)に指示する。同様に、TCサーバB(5)は、例えばLAN5aを介して1又は複数の
- 10 ユーザ端末5bに接続している。なお、LANではなく、インターネット等の他のネットワークを経由するような構成であってもよい。企業Bの社員はユーザ端末5bを操作して、書類データの受信などをTCサーバB(5)に指示する。なお、TCサーバとユーザ端末間はSSL(Secure Socket Layer Protocol)方式で暗号化している。また、本実施例では、ユーザ端末による処理については説明を省略する。
- 15

- RSPサーバ7は、送信元からの要求に基づき送信先に合わせて書類データのフォーマットなどを変換するためのフォーマット変換プログラム及びフォーマット逆変換プログラムを格納するフォーマット変換／逆変換プログラム格納部71と、受信した書類データ等を蓄積するための書類データ格納部75とを管理
- 20 している。

- 第2図に、フォーマット変換／逆変換プログラム格納部71に格納されるデータの管理テーブルの一例を示す。第2図の例では、送信先国名の列201と、フォーマット変換プログラム名の列203と、フォーマット逆変換プログラム名の列205とが含まれている。例えば、送信先国名がアメリカであれば、フォーマット変換プログラム名がUSA.exeであり、フォーマット逆変換プログラム名がUSA\_iv.exeである。送信先国名が日本であれば、フォーマット変換プログラム名がJPN.exeであり、フォーマット逆変換プログラム名が、JPN\_iv.exeである。送信先国名が英国であれば、フォーマット変換プ
- 25

プログラム名がUK. exeであり、フォーマット逆変換プログラム名がUK\_ i  
v. exeである。なお、このような管理テーブルが送信元の国ごとに設けられ  
る。なお、国毎にフォーマット変換プログラム及びフォーマット逆変換プログラ  
ムを設ける例を示したが、国ごとでなくとも、地域ごと、会社ごと等の場合もあ  
る。

以下第1図に示したシステムの処理フローを説明するが、その前に2つのコン  
ピュータ間で暗号化してデータを送信する際の処理について第3図を用いて説  
明しておく。送信元コンピュータ301から送信先コンピュータ303にオリジ  
ナル平文データ311を暗号化して送信する場合には、送信元コンピュータ30  
1は、オリジナル平文データ311に対してワンタイム共通鍵325を用いてデ  
ータ暗号化処理323を実施し、暗号化データ345を生成する。データ暗号化  
処理323には、例えばトリプルDES (Data Encryption Standard) を用いる。  
また、オリジナル平文データ311に対して例えばハッシュ関数SHA-1を用  
いたハッシュアルゴリズム313を適用し、オリジナルのハッシュ値319を生  
成する。そしてオリジナルのハッシュ値319を、送信元の秘密鍵317を用い  
て例えばRSA暗号化処理321を実施し、電子署名341を生成する。また、  
ワンタイム共通鍵325に対して、送信先の公開鍵証明書329から得られる送  
信先の公開鍵331を用いて例えばRSA暗号化処理327を実施し、暗号化さ  
れたワンタイム共通鍵347を生成する。このように生成した電子署名341と  
暗号化データ345と暗号化されたワンタイム共通鍵347を送信元の公開鍵  
証明書315と共に、例えばHTTP (Hyper Text Transfer Protocol) に従っ  
て送信先コンピュータ303に送信する。

送信先コンピュータ303は、電子署名341及び送信元の公開鍵証明書31  
5を受信すると、当該送信元の公開鍵証明書315から送信元の公開鍵355を  
取り出し、電子署名341に対してRSA復号処理351を実施し、オリジナル  
のハッシュ値353を生成する。また、暗号化データ345及び暗号化されたワ  
ンタイム共通鍵347を受信すると、当該暗号化されたワンタイム共通鍵347  
に対して送信先の秘密鍵363を用いてRSA復号処理359を実施し、ワンタ

5 イム共通鍵 3 6 1 を復元する。このワнтаイム共通鍵 3 6 1 を用いて暗号化データ 3 4 5 に対してデータ復号化処理 3 5 7 を実施し、受信した平文データ 3 6 7 を生成する。なお、送信先コンピュータ 3 0 3 には送信先の公開鍵証明書 3 2 9 が保持されており、必要に応じて送信元に送信されるようになっている。受信した平文データ 3 6 7 には、送信元で実施したのと同じハッシュアルゴリズム 3 6 9 を適用するとハッシュ値 3 7 1 が生成される。そして、オリジナルのハッシュ値 3 5 3 とハッシュ値 3 7 1 とに対する比較処理 3 7 3 により、受信した平文データがオリジナル平文 3 1 1 から改竄等が行われていないかが確認できる。すなわち、オリジナルのハッシュ値 3 5 3 とハッシュ値 3 7 1 が一致していれば改竄等  
10 等は行われておらず、一致しなければ改竄等が行われた可能性がある。もし改竄等が行われていなければ、受信した平文データを後の処理に利用することができる。

以上の処理を前提として、実施例 1 の処理の概要を第 4 図を用いて説明する。  
15 送信元のコンピュータである TC サーバ A ( 3 ) では、インボイス等の書類データ A ( 4 0 1 ) を生成し、当該書類データ A ( 4 0 1 ) に対して企業 A の電子署名 4 0 3 を生成する。そして書類データ A ( 4 0 1 ) に企業 A の電子署名 4 0 3 を付したデータを R S P サーバ 7 に送信する。この際第 3 図に示したような処理が実施される。すなわち、書類データ A ( 4 0 1 ) のハッシュ値を計算し且つ企業 A の秘密鍵で暗号化することにより企業 A の電子署名 4 0 3 を生成する。また、  
20 書類データ A ( 4 0 1 ) はワнтаイム共通鍵で暗号化され、当該ワнтаイム共通鍵も R S P の公開鍵で暗号化される。そして、暗号化された書類データ A ( 4 0 1 )、暗号化されたワнтаイム共通鍵、企業 A の公開鍵証明書及び企業 A の電子署名が R S P サーバ 7 に送信される。

25 R S P サーバ 7 では、受信時には第 3 図に示したような処理を実施する。すなわち、企業 A の公開鍵証明書から企業 A の公開鍵を得て企業 A の電子署名に対して R S A 復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワнтаイム共通鍵を R S P の秘密鍵で復号化することによりワнтаイム共通鍵を得て、暗号化された書類データ A ( 4 0 1 ) を復号化する。復号化さ

れた書類データ A (401) に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データ A (401) の送信先に合わせたフォーマット変換を  
5 フォーマット変換プログラムにより実施し、フォーマット変換された書類データ A (405) を生成する。また、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラム 407 をフォーマット変換／逆変換プログラム格納部 71 から読み出す。そして、フォーマット変換された書類データ A (405) と  
10 フォーマット逆変換プログラム 407 と企業 A の電子署名 403 とに対する R S P の電子署名 409 を生成する。すなわち、フォーマット変換された書類データ A (405) とフォーマット逆変換プログラム 407 と企業 A の電子署名 403 とからハッシュ値を計算し、R S P の秘密鍵で暗号化する。R S P サーバ 7 は、フォーマット変換された書類データ A (405) とフォーマット逆変換プログラム 407 と企業 A の電子署名 403 に R S P の電子署名 409 を付したデータ  
15 を T C サーバ B (5) に送信する。

この送信の際にも第 3 図に示したような処理を実施する。すなわち、フォーマット変換された書類データ A (405) とフォーマット逆変換プログラム 407 と企業 A の電子署名 403 とをオリジナル平文データとしてワンタイム共通鍵で暗号化し、R S P の電子署名 409 と R S P の公開鍵証明書と企業 B の公開鍵  
20 で暗号化されたワンタイム共通鍵と共に T C サーバ B (5) に送信する。なお、本実施例では企業 A の公開鍵証明書も T C サーバ B (5) に送信しなければならない場合もある。但し、企業 A の公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

T C サーバ B (5) では、受信時に第 3 図に示したような処理を実施する。す  
25 なわち、R S P の公開鍵証明書から R S P の公開鍵を得て R S P の電子署名 409 に対して R S A 復号化処理を実施し、オリジナルのハッシュ値を復元する。また、暗号化されたワンタイム共通鍵を企業 B の秘密鍵で復号化することによりワンタイム共通鍵を得て、暗号化されたデータ 403 乃至 407 を復号化する。復号化されたデータ 403 乃至 407 に対してハッシュアルゴリズムを適用する

ことによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

もし改竄等が行われていないことが確認された場合には、フォーマット逆変換プログラム407を用いて、フォーマット変換された書類データA(405)に  
5 フォーマット逆変換を施し、書類データA(411)を生成する。また、書類データA(411)にハッシュアルゴリズムを適用してハッシュ値413を計算する。一方、企業Aの公開鍵証明書から企業Aの公開鍵を取り出して、企業Aの電子署名407を当該企業Aの公開鍵で復号化するとオリジナルのハッシュ値415が復元される。よって、ハッシュ値413とハッシュ値415を比較することにより、フォーマット変換された書類データA(405)が、真正な書類データA(401)から生成されたものであるか否かが確認できるのである。  
10

以上述べた処理をまとめると第5図のようになる。TCサーバA(3)は、インボイス等の書類データを生成し、また書類データに対する企業Aの電子署名を生成し、企業Aの電子署名と書類データを、送信先の指定と共にRSPサーバ7  
15 に送信する(ステップS1)。上で述べたように第3図に示したように暗号化が行われ、企業Aの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。RSPサーバ7は、TCサーバA(3)から企業Aの電子署名と書類データと送信先の指定を受信する(ステップS3)。受信時には、第3図に示したように、書類データの復号化や、受信した書類データが改竄等されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データを  
20 書類データ格納部75に格納する。

また、送信先に合わせたフォーマット変換を実施するためのフォーマット変換プログラムをフォーマット変換/逆変換プログラム格納部71から読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換  
25 を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部75に格納する(ステップS5)。そして、実施したフォーマット変換の逆変換を行うためのフォーマット逆変換プログラムをフォーマット変換/逆変換プログラム格納部71から読み出し、当該フォーマット逆変換プログラムとフォーマット変換された書類データと企業Aの電子署名とに対してRS

- Pの電子署名を生成する。第3図及び第4図で説明したようにフォーマット逆変換プログラムとフォーマット変換された書類データと企業Aの電子署名とからハッシュ値を計算し、当該ハッシュ値をRSPの秘密鍵で暗号化する。そして、フォーマット逆変換プログラムとフォーマット変換された書類データと企業Aの電子署名とRSPの電子署名とをTCサーバB(5)に送信する(ステップS7)。送信時には第3図に示したように、当該フォーマット逆変換プログラムとフォーマット変換された書類データと企業Aの電子署名とを暗号化し、RSPの公開鍵証明書や、暗号化されたワнтаム共通鍵等と共に送信する。なお、企業Aの共通鍵証明書も送信される場合もある。
- 10 TCサーバB(5)は、RSPサーバ7からフォーマット逆変換プログラムとフォーマット変換された書類データと企業Aの電子署名とRSPの電子署名を受信する(ステップS9)。受信時には、第3図に示したように、受信したデータの復号化や、受信したデータが改竄等されていないか確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆変換プログラム
- 15 を用いて書類データに対してフォーマット逆変換を実施し、書類データを復元する(ステップS11)。この書類データは例えばメモリに格納される。但し、この復元された書類データはTCサーバA(3)で生成されたものと同一か否かはまだわからない。そして、復元された書類データからハッシュ値を生成する(ステップS13)。また、企業Aの電子署名を企業Aの公開鍵で復号化し、復号化
- 20 ハッシュ値を生成する(ステップS15)。そして、ステップS13で生成したハッシュ値とステップS15で復号した復号化ハッシュ値とを比較して、一致しているか判断する(ステップS17)。もし、一致していれば当該書類データは企業Aによる真正な書類データであり、フォーマット変換された書類データも真正な書類データとして使用することができる(ステップS19)。この書類データ
- 25 は記憶装置に格納される。一方、一致しない場合には、企業Aで作成され、企業Aで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末5bに警告を発する(ステップS21)。

このようにすれば、RSPサーバ7によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができ



るようになる。

〔実施例 2〕

実施例 1 では、R S P サーバ 7 が自らが有するフォーマット逆変換プログラム  
5 を送信先である T C サーバ B ( 5 ) へ送信するような構成であった。一方、書類  
データについては送信元たる企業 A が電子署名を作成していた。すなわち、企業  
B は、書類データについては送信元の企業 A による確証を得るが、フォーマット  
逆変換プログラムについては R S P サーバ 7 からの確証を得るのみである。場合  
によっては、フォーマット逆変換プログラムについても企業 A の確証を得るほう  
10 がよいこともある。実施例 2 は、フォーマット逆変換プログラムに送信元の確証  
を送信先の企業 B が得られるようにする場合の例を示す。

なお、第 1 図に示したシステム構成図は実施例 2 においても同じである。また、  
実施例 2 として説明するため、T C サーバ A ( 3 ) を T C サーバ E ( 3 E ) とし、  
T C サーバ B ( 5 ) を T C サーバ F ( 5 F ) として説明する。

15

まず第 6 図を用いて処理の概要を説明する。最初に、送信元のコンピュータで  
ある T C サーバ E ( 3 E ) は、R S P サーバ 7 から送信先に対応するフォーマッ  
ト逆変換プログラム 6 0 5 を取得する。この際も第 3 図に示すような処理が実施  
される。すなわち、R S P サーバ 7 は、フォーマット逆変換プログラム 6 0 5 を  
20 ワンタイム共通鍵で暗号化し、当該ワンタイム共通鍵を企業 E の公開鍵で暗号化  
する。また、フォーマット逆変換プログラム 6 0 5 のハッシュ値を所定のハッシ  
ュアルゴリズムにて計算し、当該ハッシュ値を R S P の秘密鍵で暗号化すること  
により電子署名を生成する。そして、暗号化されたフォーマット逆変換プログラ  
ム 6 0 5 と R S P の公開鍵証明書と暗号化されたワンタイム共通鍵と電子署名  
25 とを T C サーバ E ( 3 E ) に送信する。T C サーバ E ( 3 E ) は、暗号化された  
フォーマット逆変換プログラム 6 0 5 と R S P の公開鍵証明書と暗号化された  
ワンタイム共通鍵と電子署名とを受信し、企業 E の秘密鍵でワンタイム共通鍵を  
復号化する。そして、ワンタイム共通鍵でフォーマット逆変換プログラム 6 0 5  
を復号化する。また、R S P の公開鍵証明書から R S P の公開鍵を取得し、R S

Pの電子署名を復号化してオリジナルのハッシュ値を復元する。一方、プログラム逆変換プログラム605に対して所定のハッシュアルゴリズムを適用してハッシュ値を計算する。これらのハッシュ値を比較することにより、改竄等が行われなかったか否かを判断する。

- 5      もし、改竄等が行われていない場合には、フォーマット逆変換プログラム605に対する企業Eの電子署名2(607)を生成する。すなわち、フォーマット逆変換プログラム605に対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、そのハッシュ値を企業Eの秘密鍵で暗号化する。さらにTCサーバE(3E)は、インボイス等の書類データB(601)を生成し、当該書類
- 10    データB(601)に対して企業Eの電子署名を生成する。すなわち、書類データB(601)から所定のハッシュアルゴリズムに従ってハッシュ値を計算し、そのハッシュ値を企業Eの秘密鍵で暗号化する。

- そして書類データB(601)に企業Eの電子署名1(603)を付したデータ及びフォーマット逆変換プログラム605に企業Eの電子署名2(607)を
- 15    付したデータをRSPサーバ7に送信する。この際第3図に示したような処理が実施される。すなわち、書類データB(601)のハッシュ値を計算し且つ企業Eの秘密鍵で暗号化することにより企業Eの電子署名1(603)を生成する。また、書類データB(601)はワンタイム共通鍵で暗号化され、当該ワンタイム共通鍵もRSPの公開鍵で暗号化される。さらに、フォーマット逆変換プログラム605のハッシュ値を計算し且つ企業Eの秘密鍵で暗号化することにより
- 20    企業Eの電子署名2(607)を生成する。また、フォーマット逆変換プログラム605はワンタイム共通鍵で暗号化される。そして、暗号化された書類データB(601)、暗号化されたワンタイム共通鍵、企業Eの公開鍵証明書、暗号化されたフォーマット逆変換プログラム605、企業Eの電子署名1(603)及び
- 25    企業Eの電子署名2(607)がRSPサーバ7に送信される。

RSPサーバ7では、受信時には第3図に示したような処理を実施する。すなわち、企業Eの公開鍵証明書から企業Eの公開鍵を得て企業Eの電子署名1(603)に対してRSA復号化処理を実施し、オリジナルのハッシュ値 $\alpha 1$ を復元する。また、暗号化されたワンタイム共通鍵をRSPの秘密鍵で復号化すること

によりワンタイム共通鍵を得て、暗号化された書類データ B (601) を復号化する。復号化された書類データ B (601) に対してハッシュアルゴリズムを適用することによりハッシュ値  $\beta 1$  を計算し、オリジナルのハッシュ値  $\alpha 1$  と比較することにより改竄等が行われていないことを確認する。同様に、企業 E の公開鍵を得て企業 E の電子署名 2 (605) に対して RSA 復号化処理を実施し、オリジナルのハッシュ値  $\alpha 2$  を復元する。また暗号化されたフォーマット逆変換プログラム 605 をワンタイム共通鍵でもって復号化する。フォーマット逆変換プログラム 605 に対して所定のハッシュアルゴリズムにてハッシュ値  $\beta 2$  を計算し、オリジナルのハッシュ値  $\alpha 2$  と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データ B (601) の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データ B (609) を生成する。また、フォーマット変換された書類データ B (609) とフォーマット逆変換プログラム 605 と企業 E の電子署名 2 (607) と企業 E の電子署名 1 (603) とに対する RSP の電子署名 611 を生成する。すなわち、フォーマット変換された書類データ B (609) とフォーマット逆変換プログラム 605 と企業 E の電子署名 2 (607) と企業 E の電子署名 1 (603) とからハッシュ値を計算し、RSP の秘密鍵で暗号化する。RSP サーバ 7 は、フォーマット変換された書類データ B (609) とフォーマット逆変換プログラム 605 と企業 E の電子署名 2 (607) と企業 E の電子署名 1 (603) RSP の電子署名 611 を付したデータを TC サーバ F (5F) に送信する。

この送信の際にも第 3 図に示したような処理を実施する。すなわち、フォーマット変換された書類データ B (609) とフォーマット逆変換プログラム 605 と企業 E の電子署名 2 (607) と企業 E の電子署名 1 (603) をオリジナル平文データとしてワンタイム共通鍵で暗号化し、RSP の電子署名 611 と RSP の公開鍵証明書と企業 F の公開鍵で暗号化されたワンタイム共通鍵と共に TC サーバ F (5F) に送信する。なお、本実施例では企業 E の公開鍵証明書も TC サーバ F (5F) に送信しなければならない場合もある。但し、企業 E の公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

TCサーバF (5F) では、受信時に第3図に示したような処理を実施する。  
すなわち、RSPの公開鍵証明書からRSPの公開鍵を得てRSPの電子署名6  
11に対してRSA復号化処理を実施し、オリジナルのハッシュ値を復元する。  
また、暗号化されたワнтаム共通鍵を企業Fの秘密鍵で復号化することにより  
5 ワнтаム共通鍵を得て、暗号化されたデータ603乃至609を復号化する。  
復号化されたデータ603乃至609に対してハッシュアルゴリズムを適用す  
ることによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

もし改竄等が行われていないことが確認された場合には、さらにフォーマット  
10 逆変換プログラム605から所定のハッシュアルゴリズムにてハッシュ値61  
3を計算し、企業Eの電子署名2(607)を企業Eの公開鍵で復号化し、オリ  
ジナルのハッシュ値615を復元する。そして、計算されたハッシュ値613と  
オリジナルのハッシュ値615を比較することにより、フォーマット逆変換プロ  
グラム605が企業Eが認定した逆変換プログラムであるかどうかを確認する。

15 もし、フォーマット逆変換プログラム605が企業Eが認定した逆変換プロ  
グラムであるということが確認されると、フォーマット変換された書類データ(6  
09)をフォーマット逆変換プログラム605を用いて書類データB(617)  
を生成する。そして、書類データB(617)から所定のハッシュアルゴリズム  
にてハッシュ値619を生成する。一方、企業Eの公開鍵証明書から企業Eの公  
20 開鍵を取り出して、企業Eの電子署名1(603)を当該企業Eの公開鍵で復  
号化するとオリジナルのハッシュ値621が復元される。よって、ハッシュ値61  
9とハッシュ値621を比較することにより、フォーマット変換された書類デー  
タ609が、真正な書類データB(601)から生成されたものであるか否か、  
すなわち企業Eで作成され、企業Eで認定した変換プログラムでフォーマット変  
25 換された書類データであるか否かが確認できるのである。

次に第7図を用いて実施例2の処理フローを説明する。最初に、TCサーバE  
(3E)は、送信先の指定を含むフォーマット逆変換プログラムの送信要求をR  
SPサーバ7に送信する(ステップS31)。送信先の指定は、送信先を特定し

- たものであっても良いし、送信先のグループ、例えば国などを指定するような形であってても良い。RSPサーバ7は、TCサーバE（3E）から送信先の指定を含むフォーマット逆変換プログラムの送信要求を受信すると（ステップS33）、送信先に対応するフォーマット逆変換プログラムをフォーマット変換／逆変換
- 5 プログラム格納部71から抽出し、TCサーバE（3E）へ送信する（ステップS35）。なお、フォーマット逆変換プログラムは、送信元と送信先とで特定される場合もあり、その場合には送信元及び送信先に対応するフォーマット逆変換プログラムをフォーマット変換／逆変換プログラム格納部71から読み出すようにする。第3図に示したようにフォーマット逆変換プログラムの暗号化が行われ、RSPの電子署名と、RSPの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信される。
- 10

- TCサーバE（3E）は、RSPサーバ7から送信先に対応するフォーマット逆変換プログラムを受信する（ステップS37）。第3図に示したように、ワンタイム共通鍵を復号化し、当該ワンタイム共通鍵を用いてフォーマット逆変換プログラムを復号化する。さらに、フォーマット逆変換プログラムからハッシュ値を計算し、RSPの電子署名からオリジナルのハッシュ値を復元し、比較することにより改竄等が行われていないことを確認する。そして改竄等が行われていない場合には、書類データに対して企業Eの電子署名1を生成し、フォーマット逆変換プログラムに対して企業Eの電子署名2を生成する。そして、書類データと
- 15
- 20 当該書類データに対する企業Eの電子署名1とフォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する企業Eの電子署名2をRSPサーバ7に送信する（ステップS39）。この際再度送信先の情報を送信するようにしても良い。ここでも第3図のような処理が実施される。すなわち、書類データに対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、企業E
- 25
- の秘密鍵にて暗号化することにより企業Eの電子署名1を生成し、フォーマット逆変換プログラムに対して所定のハッシュアルゴリズムを適用してハッシュ値を計算し、企業Eの秘密鍵にて暗号化することにより企業Eの電子署名2を生成する。また、書類データ及びフォーマット逆変換プログラムについてはワンタイム共通鍵で暗号化し、ワンタイム共通鍵をRSPの公開鍵で暗号化する。そして、

企業Eの公開鍵証明書と共にRSPサーバ7に送信する。

RSPサーバ7は、TCサーバE（3E）から企業Eの電子署名1と書類データと企業Eの電子署名2とフォーマット逆変換プログラムとを受信する（ステップS41）。受信時には、第3図に示したように、書類データの復号化や、受信した書類データが改竄等されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データ格納部75に格納される。また、暗号化されたフォーマット逆変換プログラムの復号化や、受信したフォーマット逆変換プログラムが改竄等されていないか確認する処理を実施する。

そしてRSPサーバ7は、フォーマット変換を行うためフォーマット変換／逆変換プログラム格納部71から送信先に対応するフォーマット変換プログラムを読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部75に格納する（ステップS43）。そして、受信したフォーマット逆変換プログラムと企業Eの電子署名2とフォーマット変換された書類データと企業Eの電子署名2とに対してRSPの電子署名を生成する。第3図及び第6図で説明したようにフォーマット逆変換プログラムと企業Eの電子署名2とフォーマット変換された書類データと企業Eの電子署名1とからハッシュ値を計算し、当該ハッシュ値をRSPの秘密鍵で暗号化する。そして、フォーマット逆変換プログラムと企業Eの電子署名2とフォーマット変換された書類データと企業Eの電子署名1とRSPの電子署名とをTCサーバF（5F）に送信する（ステップS45）。送信時には第3図に示したように、当該フォーマット逆変換プログラムと企業Eの電子署名2とフォーマット変換された書類データと企業Eの電子署名1とを暗号化し、RSPの公開鍵証明書や、暗号化されたワンタイム共通鍵等と共に送信する。なお、企業Eの共通鍵証明書も送信される場合もある。

TCサーバF（5F）は、RSPサーバ7からフォーマット逆変換プログラムと企業Eの電子署名2とフォーマット変換された書類データと企業Eの電子署名2とRSP電子署名を受信する（ステップS47）。受信時には、第3図に示したように、受信したデータの復号化や、受信したデータが改竄等されていない

か確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆変換プログラムに対して所定のハッシュアルゴリズムを適用してハッシュ値を生成し、企業Eの電子署名2をRSPの公開鍵で復号化することにより復号化ハッシュ値を生成する（ステップS49）。そして、生成したハッシュ値と復号化ハッシュ値を比較し、フォーマット逆変換プログラムが送信元が想定しているフォーマット逆変換プログラムであるかを確認する（ステップS51）。もし、生成したハッシュ値と復号化ハッシュ値とが一致していない場合には、送信元が想定していないフォーマット逆変換プログラムであるからステップS63に移行して、企業Eで認定した逆変換プログラムとして認められない旨の警告を発する。

一方、ステップS51で一致していると判断された場合には、当該フォーマット逆変換プログラムを用いて書類データに対してフォーマット逆変換を実施し、書類データを復元する（ステップS53）。当該書類データを例えばメモリに格納する。但し、この復元された書類データはTCサーバE（3E）で生成されたものと同一か否かはまだわからない。そして、復元された書類データからハッシュ値2を生成する（ステップS55）。また、企業Eの電子署名1を企業Eの公開鍵で復号化し、復号化ハッシュ値2を生成する（ステップS57）。そして、ステップS55で生成したハッシュ値2とステップS57で復号した復号化ハッシュ値2とを比較して、一致しているか判断する（ステップS59）。もし、一致していれば当該書類データは企業Eによる真正な書類データであり、フォーマット変換された書類データも真正な書類として使用することができる（ステップS61）。書類データは記憶装置に格納される。一方、一致しない場合には、企業Eで作成され、企業Eで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末5bに警告を発する（ステップS63）。

このようにすれば、RSPサーバ7によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができるようになる。また、TCサーバF（5F）において実行されるフォーマット逆

変換プログラムも送信元の想定したフォーマット逆変換プログラムであることが確認できるため、TCサーバF（5F）では安心して実行することができる。

- なお、ステップS39においてフォーマット逆変換プログラムをTCサーバE（3E）からRSPサーバ7へ送信しない場合もある。また、フォーマット逆変換プログラムと書類データとに対して別々に企業Eの電子署名を生成していたが、一括して企業Eの電子署名を生成することもある。

### 〔実施例3〕

- 実施例1及び実施例2では、フォーマット逆変換プログラムをRSPサーバから送信先のTCサーバに送信する構成であったが、送信先がフォーマット逆変換プログラムのセットを保持しており且つ送信先で実行すべきフォーマット逆変換プログラムを特定できれば、書類データの送信の都度にフォーマット逆変換プログラムを送信する必要はなくなる。実施例3では、送信先がフォーマット逆変換プログラムのセットを保持している場合の例を説明する。

15

- 本発明の実施例3に係るシステム概要図を第8図に示す。コンピュータ・ネットワークであるインターネット11には、例えばインボイス等の書類データの送信元である企業Cが管理・運用しているTCサーバC（13）と、例えば書類データのフォーマット変換や書類データの蓄積サービスなどを提供するためのRSPサーバ17と、例えば書類データの送信先である企業Dが管理・運営しているTCサーバD（15）とが接続されている。なお、TCサーバは2つだけでなく多数インターネット11に接続されている。また、RSPサーバ17も1つだけでなく複数存在している場合もある。

- TCサーバC（13）は、例えばLAN（Local Area Network）13aを介して1又は複数のユーザ端末13bに接続している。なお、LANではなく、インターネット等の他のネットワークを経由する構成であってもよい。企業Cの社員はユーザ端末13bを操作して、書類データの送信などをTCサーバC（13）に指示する。また、TCサーバC（13）は、フォーマット逆変換プログラムを格納するフォーマット逆変換プログラム格納部13cを管理している。同様に、

25



TCサーバD (15) は、例えばLAN 15 a を介して1又は複数のユーザ端末15 b に接続している。なお、LANではなくインターネット等の他のネットワークを経由するような構成であってもよい。企業Dの社員はユーザ端末15 b を操作して、書類データの受信などをTCサーバD (15) に指示する。同様に、

5 TCサーバD (15) は、フォーマット逆変換プログラムを格納するフォーマット逆変換プログラム格納部15 c を管理している。なお、本実施例では、ユーザ端末による処理については説明を省略する。

RSPサーバ17は、送信元からの要求に基づき送信先に合わせて書類データのフォーマットなどを変換するためのフォーマット変換プログラムを格納する

10 フォーマット変換プログラム格納部171と、受信した書類データ等を蓄積するための書類データ格納部175とを管理している。

第9図に、フォーマット逆変換プログラム格納部13 c 及び15 c に格納されるデータの管理テーブルの一例を示す。第9図の例では、フォーマット逆変換プログラムIDの列901と、フォーマット逆変換プログラム名の列903とが含まれている。例えば、送信元国名がアメリカの場合にはUSAというフォーマット逆変換プログラムIDを与えて、そのIDに対応するフォーマット逆変換プログラム名をUSA\_\_iv.exeとする。送信元国名が日本の場合にはJPNというフォーマット逆変換プログラムIDを与えて、フォーマット逆変換プログラム名をJPN\_\_iv.exeとする。送信元国名が英国の場合にはUKというフォーマット逆変換プログラムIDを与えて、フォーマット逆変換プログラム名をUK\_\_iv.exeとする。なお、国毎にフォーマット逆変換プログラムを設ける例を示したが、国ごとでなくとも、地域ごと、会社ごと等の場合もある。

15

20

なお、フォーマット変換プログラム格納部171には、送信先国名に対応して

25 フォーマット変換プログラム名が格納された管理テーブルが設けられる。なお、送信元国名毎にこの管理テーブルが設けられるが、管理テーブルに対応してフォーマット逆変換プログラムIDが格納されている。なお、国ごとでなく、地域ごと、会社ごとなどであっても良い。

次に実施例3の処理の概要を第10図を用いて説明する。送信元のコンピュータであるTCサーバC(13)では、インボイス等の書類データC(1001)を生成し、当該書類データC(1001)に対して企業Cの電子署名を生成する。そして書類データC(1001)に企業Cの電子署名1003を付したデータを  
5 RSPサーバ17に送信する。この際第3図に示したような処理が実施される。すなわち、書類データC(1001)のハッシュ値を計算し且つ企業Cの秘密鍵で暗号化することにより企業Cの電子署名1003を生成する。また、書類データC(1001)はワнтаム共通鍵で暗号化され、当該ワнтаム共通鍵もRSPの公開鍵で暗号化される。そして、暗号化された書類データC(1001)、  
10 暗号化されたワнтаム共通鍵、企業Cの公開鍵証明書及び企業Cの電子署名1003がRSPサーバ17に送信される。

RSPサーバ17では、受信時には第3図に示したような処理を実施する。すなわち、企業Cの公開鍵証明書から企業Cの公開鍵を得て企業Cの電子署名1003に対してRSA復号化処理を実施し、オリジナルのハッシュ値を復元する。  
15 また、暗号化されたワнтаム共通鍵をRSPの秘密鍵で復号化することによりワнтаム共通鍵を得て、暗号化された書類データC(1001)を復号化する。復号化された書類データC(1001)に対してハッシュアルゴリズムを適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較することにより改竄等が行われていないことを確認する。

その後、当該書類データC(1001)の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データC(1005)を生成する。そして、フォーマット変換された書類データC(1005)とフォーマット逆変換プログラムID1007と企業Cの電子署名1003とに対するRSPの電子署名1009を生成する。すなわち、フォーマット  
25 変換された書類データC(1005)とフォーマット逆変換プログラムID1007と企業Cの電子署名1003とからハッシュ値を計算し、RSPの秘密鍵で暗号化する。RSPサーバ17は、フォーマット変換された書類データC(1005)とフォーマット逆変換プログラムID1007と企業Cの電子署名1003にRSPの電子署名1009を付したデータをTCサーバD(15)に送信す

る。

なお、フォーマット逆変換プログラムID1007に対してはRSPの電子署名を生成しない場合もある。すなわち、送信元の情報（例えば送信元の国名や会社識別子、ネットワークにおけるアドレスなど）をフォーマット逆変換プログラムIDとして用いる場合には、あえてフォーマット逆変換プログラムID1007に対してRSPの電子署名を生成する必要がない場合もある。このような場合には、当該書類データC（1001）の送信先に合わせたフォーマット変換をフォーマット変換プログラムにより実施し、フォーマット変換された書類データC（1005）を生成する。また、フォーマット逆変換プログラムID1007を

5     フォーマット変換プログラム格納部171から読み出す。そして、フォーマット変換された書類データC（1005）と企業Cの電子署名1003とに対するRSPの電子署名1009を生成する。すなわち、フォーマット変換された書類データC（1005）と企業Cの電子署名1003とからハッシュ値を計算し、RSPの秘密鍵で暗号化する。RSPサーバ17は、フォーマット変換された書類

10    データC（1005）と企業Cの電子署名1003にRSPの電子署名1009及びフォーマット逆変換プログラムID1007を付したデータをTCサーバD（15）に送信する。

この送信の際にも第3図に示したような処理を実施する。すなわち、上で述べた第1の例（a）の場合には、フォーマット変換された書類データC（1005）

20    とフォーマット逆変換プログラムID1007と企業Cの電子署名1003とをオリジナル平文データとしてワнтаイム共通鍵で暗号化し、RSPの電子署名1009とRSPの公開鍵証明書と企業Dの公開鍵で暗号化されたワнтаイム共通鍵と共にTCサーバD（15）に送信する。なお、本実施例では企業Cの公開鍵証明書もTCサーバD（15）に送信しなければならない場合もある。但し、

25    企業Cの公開鍵証明書が別の手段で取得できるようになっていれば送信しなくともよい。

上で述べた第2の例（b）の場合には、フォーマット変換された書類データC（1005）と企業Cの電子署名1003とをオリジナル平文データとしてワнтаイム共通鍵で暗号化し、フォーマット逆変換プログラムID1006とRSP

の電子署名 1009 と R S P の公開鍵証明書と企業 D の公開鍵で暗号化された  
ワнтаイム共通鍵と共に T C サーバ D (15) に送信する。

- T C サーバ D (15) では、受信時に第 3 図に示したような処理を実施する。  
すなわち、R S P の公開鍵証明書から R S P の公開鍵を得て R S P の電子署名 1  
5 009 に対して R S A 復号化処理を実施し、オリジナルのハッシュ値を復元する。  
また、暗号化されたワнтаイム共通鍵を企業 D の秘密鍵で復号化することにより  
ワнтаイム共通鍵を得て、暗号化されたデータ 1003 乃至 1007 を復号化する。  
復号化されたデータ 1003 乃至 1007 に対してハッシュアルゴリズムを  
適用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較するこ  
10 とにより改竄等が行われていないことを確認する。上で述べた第 2 の例の場合に  
は、R S P の公開鍵証明書から R S P の公開鍵を得て R S P の電子署名 1009  
に対して R S A 復号化処理を実施し、オリジナルのハッシュ値を復元する。また、  
暗号化されたワнтаイム共通鍵を企業 D の秘密鍵で復号化することによりワ  
ンタイム共通鍵を得て、暗号化されたデータ 1003 及び 1005 を復号化する。  
15 復号化されたデータ 1003 及び 1005 に対してハッシュアルゴリズムを適  
用することによりハッシュ値を計算し、オリジナルのハッシュ値と比較するこ  
とにより改竄等が行われていないことを確認する。

- もし改竄等が行われていないことが確認された場合には、フォーマット逆変換  
プログラム I D 1007 を用いてフォーマット逆変換プログラム格納部 15 c  
20 から対応するフォーマット逆変換プログラムを抽出する。そして当該フォー  
マット逆変換プログラムを用いて、フォーマット変換された書類データ C (1005)  
にフォーマット逆変換を施し、書類データ C (1013) を生成する。また、書  
類データ C (1013) にハッシュアルゴリズムを適用してハッシュ値 1017  
を計算する。一方、企業 C の公開鍵証明書から企業 C の公開鍵を取り出して、  
25 企業 C の電子署名 1003 を当該企業 C の公開鍵で復号化するとオリジナルのハ  
ッシュ値 1015 が復元される。よって、ハッシュ値 1017 とハッシュ値 10  
15 を比較することにより、フォーマット変換された書類データ C (1005)  
が、真正な書類データ C (1001) から生成されたものであることが確認でき  
るのである。

以上述べた処理をまとめると第11図のようになる。TCサーバC(13)は、インボイス等の書類データを生成し、また書類データに対する企業Cの電子署名を生成し、企業Cの電子署名と書類データを、送信先の指定と共にRSPサーバ17に送信する(ステップS71)。なお、送信元の情報(例えば識別情報など)も送信される。上で述べたように第3図に示したように暗号化が行われ、企業Cの公開鍵証明書や、暗号化されたワнтаム共通鍵等と共に送信される。RSPサーバ17は、TCサーバC(13)から企業Cの電子署名と書類データと送信先の指定を受信する(ステップS73)。送信元の情報も受信する。受信時には、第3図に示したように、書類データの復号化や、受信した書類データが改竄等  
5  
10  
15  
20  
25

されていないか確認する処理を実施し、改竄等がなされていないことが確認されると書類データ格納部75に格納される。

また、送信先に合わせたフォーマット変換を実施するためのフォーマット変換プログラムをフォーマット変換プログラム格納部171から読み出し、当該フォーマット変換プログラムを用いて書類データに対してフォーマット変換を実施することにより、フォーマット変換された書類データを生成し、例えば書類データ格納部75に格納する(ステップS75)。そして、実施したフォーマット変換の逆変換を行うためのフォーマット逆変換プログラムのIDを例えば送信元の情報に基づきフォーマット変換プログラム格納部171から読み出し、当該フォーマット逆変換プログラムIDとフォーマット変換された書類データと企業Cの電子署名とに対してRSPの電子署名を生成する。上で述べたようにフォーマット変換された書類データと企業Cの電子署名とに対してRSPの電子署名を生成する場合もある。第3図及び第10図で説明したようにフォーマット逆変換プログラムIDとフォーマット変換された書類データと企業Cの電子署名とからハッシュ値を計算し、当該ハッシュ値をRSPの秘密鍵で暗号化する。フォーマット変換された書類データと企業Cの電子署名とからハッシュ値を計算し、当該ハッシュ値をRSPの秘密鍵で暗号化する場合もある。そして、フォーマット逆変換プログラムIDとフォーマット変換された書類データと企業Cの電子署名とRSPの電子署名とをTCサーバD(15)に送信する(ステップS77)。送信時には第3図に示したように、当該フォーマット逆変換プログラムIDとフ

フォーマット変換された書類データと企業Cの電子署名とを暗号化し、RSPの公開鍵証明書や、暗号化されたワнтаム共通鍵等と共に送信される。上で述べたようにフォーマット逆変換プログラムIDについては暗号化しないで送信する場合もある。なお、企業Cの共通鍵証明書も送信される場合もある。

- 5 TCサーバD(15)は、RSPサーバ17からフォーマット逆変換プログラムIDとフォーマット変換された書類データと企業Cの電子署名とRSPの電子署名とを受信する(ステップS79)。受信時には、第3図に示したように、受信したデータの復号化や、受信したデータが改竄等されていないか確認する処理を実施する。改竄等が実施されていないことが確認されると、フォーマット逆
- 10 変換プログラムIDを用いてフォーマット逆変換プログラム格納部15cから対応するフォーマット逆変換プログラムを取り出し、書類データに対してフォーマット逆変換を実施し、書類データを復元する(ステップS81)。復元されたデータはメモリに格納される。但し、この復元された書類データはTCサーバC
- 15 (13)で生成されたものと同じか否かはまだわからない。そして、復元された書類データからハッシュ値を生成する(ステップS83)。また、企業Cの電子署名を企業Cの公開鍵で復号化し、復号化ハッシュ値を生成する(ステップS85)。そして、ステップS83で生成したハッシュ値とステップS85で復号した復号化ハッシュ値とを比較して、一致しているか判断する(ステップS87)。もし、一致していれば当該書類データは企業Cによる真正な書類データであり、
- 20 フォーマット変換された書類データも真正な書類として使用することができる(ステップS89)。書類データは例えば記憶装置に格納される。一方、一致しない場合には、企業Cで作成され、企業Cで認定した変換プログラムでフォーマット変換された書類データとして認められず、例えばユーザ端末15bに警告を発する(ステップS91)。
- 25 このようにすれば、RSPサーバ17によりフォーマット変換が施されても元の書類データが送信元による真正な書類データであることを確認することができるようになる。

以上本発明の実施例を説明したが、本発明は上で述べた実施例に限定されない。

- 例えば、TCサーバやRSPサーバといった名称は一例であって他の名称でも同様の機能を有するコンピュータであってもよい。また、TCサーバやRSPサーバは一台のコンピュータではなく複数のコンピュータにて実施することができる。また、公開鍵暗号の方法としてはRSAを用いる例を示したが、他のEIGamalや楕円又は超楕円暗号を用いることも可能である。共通鍵暗号もDESでなくともよい。フォーマット変換として説明したが、フォーマット以外の変換も含まれるものとする。
- 5

## 請求の範囲

1. 第1のコンピュータから第1のデータと少なくとも当該第1のデータに対する第1の電子署名とを受信する受信ステップと、
- 5 前記受信ステップにおいて受信された前記第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成するフォーマット変換ステップと、  
少なくとも前記フォーマット変換ステップにおいて生成された前記第2のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第1の電子署名とを前記送信先に関連する第2のコンピュータ  
10 に送信する送信ステップと、  
を含む情報処理方法。
2. 少なくとも前記フォーマット変換ステップにおいて生成された前記第2のデータと前記フォーマット逆変換プログラムと前記第1の電子署名とに対する第2の電子署名を生成する電子署名生成ステップ  
15 をさらに含み、  
前記送信ステップにおいて、前記第2の電子署名をさらに前記第2のコンピュータに送信する
- 20 ことを特徴とする請求項1記載の情報処理方法。
3. 前記受信ステップにおいて、少なくとも前記フォーマット逆変換プログラムに対する第3の電子署名をさらに受信する、  
ことを特徴とする請求項1記載の情報処理方法。
- 25 4. 前記フォーマット変換ステップにおいて生成された前記第2のデータと前記フォーマット逆変換プログラムと前記第3の電子署名と前記第1の電子署名とに対する第4の電子署名を生成する電子署名生成ステップ  
をさらに含み、



前記送信ステップにおいて、前記第 3 の電子署名及び前記第 4 の電子署名をさらに前記第 2 のコンピュータに送信する

ことを特徴とする請求項 3 記載の情報処理方法。

- 5 5. 前記第 1 のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信するステップと、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第 1 のコンピュータに送信するステップと、

- 10 をさらに含む請求項 3 記載の情報処理方法。

6. 前記受信ステップにおいて、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第 3 の電子署名とを受信する、

ことを特徴とする請求項 1 記載の情報処理方法。

15

7. 第 1 のコンピュータから第 1 のデータと少なくとも当該第 1 のデータに対する第 1 の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第 1 のデータに対して当該第 1 のデータの送信先に対応するフォーマット変換を実施し、第 2 のデータを生成する

- 20 フォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第 2 のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第 1 の電子署名とを前記送信先に関連する第 2 のコンピュータに送信する送信ステップと、

- 25 を含む情報処理方法。

8. 少なくとも前記フォーマット変換ステップにおいて生成された前記第 2 のデータと前記第 1 の電子署名とに対する第 2 の電子署名を生成する電子署名生成ステップ

をさらに含み、

前記送信ステップにおいて、前記第 2 の電子署名をさらに前記第 2 のコンピュータに送信する

ことを特徴とする請求項 7 記載の情報処理方法。

5

9. 前記電子署名生成ステップが、

少なくとも前記フォーマット変換ステップにおいて生成された前記第 2 のデータと前記フォーマット逆変換プログラムを識別するための情報と前記第 1 の電子署名とに対する第 2 の電子署名を生成するステップである、

10 ことを特徴とする請求項 8 記載の情報処理方法。

10. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、

15 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、

20 を含む情報処理方法。

11. 前記送信ステップにおいて、

生成された前記電子署名と前記データと当該データに対する電子署名と前記フォーマット逆変換プログラムとを前記データのフォーマット変換を実施する  
25 コンピュータに送信する

ことを特徴とする請求項 10 記載の情報処理方法。

12. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換

プログラムの送信要求を送信するステップと、

- 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記
- 5 電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、
- を含む情報処理方法。

- 1 3. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、
- 10

受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

- 少なくとも前記逆変換データから第1ハッシュ値を計算するステップと、
- 15 受信された前記電子署名から第2ハッシュ値を復元するステップと、
- 計算された前記第1ハッシュ値と復元された前記第2ハッシュ値とを比較して改竄の有無を判断するステップと、
- を含む情報処理方法。

- 20 1 4. 前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムとに対する電子署名をさらに受信することを特徴とする請求項1 3記載の情報処理方法。

- 25 1 5. 前記受信ステップにおいて、前記フォーマット逆変換プログラムに対する第2の電子署名を受信し、
- 前記プログラム逆変換プログラムから第3ハッシュ値を計算するステップと、
- 前記第2の電子署名から第4ハッシュ値を復元するステップと、
- 計算された前記第3ハッシュ値と復元された前記第4ハッシュ値とを比較し

て改竄の有無を判断するステップと、

をさらに含む請求項 1 3 記載の情報処理方法。

5 1 6. 前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムと前記フォーマット逆変換プログラムに対する第 2 の電子署名とに対する電子署名をさらに受信することを特徴とする請求項 1 5 記載の情報処理方法。

10 1 7. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、

15 受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、

抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

前記逆変換データから第 1 ハッシュ値を計算するステップと、

受信された前記電子署名から第 2 ハッシュ値を復元するステップと、

20 計算された前記第 1 ハッシュ値と復元された前記第 2 ハッシュ値とを比較して改竄の有無を判断するステップと、

を含む情報処理方法。

25 1 8. 前記受信ステップにおいて、前記フォーマット変換されたデータと前記少なくともフォーマット変換前のデータに対する電子署名と前記フォーマット逆変換プログラムを識別するための識別情報と前記フォーマット逆変換プログラムに対する第 2 の電子署名とに対する電子署名をさらに受信することを特徴とする請求項 1 7 記載の情報処理方法。

19. 第1のコンピュータから第1のデータと少なくとも当該第1のデータに対する第1の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成する

5 フォーマット変換ステップと、

少なくとも前記フォーマット変換ステップにおいて生成された前記第2のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第1の電子署名とを前記送信先に関連する第2のコンピュータに送信する送信ステップと、

10 をコンピュータに実行させるためのプログラム。

20. 前記受信ステップにおいて、少なくとも前記フォーマット逆変換プログラムに対する第3の電子署名をさらに受信する、

ことを特徴とする請求項19記載のプログラム。

15

21. 前記第1のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信するステップと、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第1のコンピュータに送信するステップ

20 と、

をさらにコンピュータに実行させるための請求項20記載のプログラム。

22. 前記受信ステップにおいて、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第3の電子署名とを受信する、

25 ことを特徴とする請求項19記載のプログラム。

23. 第1のコンピュータから第1のデータと少なくとも当該第1のデータに対する第1の電子署名とを受信する受信ステップと、

前記受信ステップにおいて受信された前記第1のデータに対して当該第1の

データの送信先に対応するフォーマット変換を実施し、第 2 のデータを生成するフォーマット変換ステップと、

- 少なくとも前記フォーマット変換ステップにおいて生成された前記第 2 のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第 1 の電子署名とを前記送信先に関連する第 2 のコンピュータに送信する送信ステップと、  
5 をコンピュータに実行させるためのプログラム。

24. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、  
10

- 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、  
15 をコンピュータに実行させるためのプログラム。

25. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信するステップと、  
20

- 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信ステップと、  
25 をコンピュータに実行させるためのプログラム。

26. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変

換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、

- 5      少なくとも前記逆変換データから第1ハッシュ値を計算するステップと、  
受信された前記電子署名から第2ハッシュ値を復元するステップと、  
計算された前記第1ハッシュ値と復元された前記第2ハッシュ値とを比較して改竄の有無を判断するステップと、  
をコンピュータに実行させるためのプログラム。

10

27. 前記受信ステップにおいて、前記フォーマット逆変換プログラムに対する第2の電子署名を受信し、

前記プログラム逆変換プログラムから第3ハッシュ値を計算するステップと、  
前記第2の電子署名から第4ハッシュ値を復元するステップと、

- 15      計算された前記第3ハッシュ値と復元された前記第4ハッシュ値とを比較して改竄の有無を判断するステップと、  
をさらにコンピュータに実行させる請求項26記載のプログラム。

28. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信ステップと、

受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出するステップと、

- 25      抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成するステップと、  
前記逆変換データから第1ハッシュ値を計算するステップと、  
受信された前記電子署名から第2ハッシュ値を復元するステップと、  
計算された前記第1ハッシュ値と復元された前記第2ハッシュ値とを比較し

て改竄の有無を判断するステップと、

をコンピュータに実行させるためのプログラム。

29. 第1のコンピュータから第1のデータと少なくとも当該第1のデータに対  
5 する第1の電子署名とを受信する受信手段と、

前記受信手段により受信された前記第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成するフォーマット変換手段と、

- 10 少なくとも前記フォーマット変換手段により生成された前記第2のデータと  
前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムと前記第1の電子署名とを前記送信先に関連する第2のコンピュータに送信する送信手段と、

を有するコンピュータ・システム。

- 15 30. 前記受信手段が、少なくとも前記フォーマット逆変換プログラムに対する第3の電子署名をさらに受信する、

ことを特徴とする請求項29記載のコンピュータ・システム。

- 20 31. 前記第1のコンピュータから送信先の指定を含む前記フォーマット逆変換プログラムの送信要求を受信する手段と、

前記送信先に対応する前記フォーマット逆変換プログラムを、フォーマット逆変換プログラム格納部から抽出し、前記第1のコンピュータに送信する手段と、  
をさらに有する請求項30記載のコンピュータ・システム。

- 25 32. 前記受信手段が、前記フォーマット逆変換プログラムと当該フォーマット逆変換プログラムに対する第3の電子署名とを受信する、

ことを特徴とする請求項29記載のコンピュータ・システム。

33. 第1のコンピュータから第1のデータと少なくとも当該第1のデータに対



する第1の電子署名とを受信する受信手段と、

前記受信ステップにおいて受信された前記第1のデータに対して当該第1のデータの送信先に対応するフォーマット変換を実施し、第2のデータを生成するフォーマット変換手段と、

- 5      少なくとも前記フォーマット変換ステップにおいて生成された前記第2のデータと前記フォーマット変換の逆変換を実施するためのフォーマット逆変換プログラムを識別するための識別情報と前記第1の電子署名とを前記送信先に関連する第2のコンピュータに送信する送信手段と、
- を有するコンピュータ・システム。

10

34. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信する手段と、

- 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラムに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データと当該データに対する電子署名とを前記データのフォーマット変換を実施するコンピュータに送信する送信手段と、
- 15      を有するコンピュータ・システム。

20

35. データのフォーマット変換を実施するコンピュータに対して、データの送信先の指定を含む、フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムの送信要求を送信する手段と、

- 前記データのフォーマット変換を実施するコンピュータから前記フォーマット逆変換プログラムを受信した場合には、少なくとも前記フォーマット逆変換プログラム及び前記データに対する電子署名を生成し、少なくとも生成された前記電子署名と前記データとを前記データのフォーマット変換を実施するコンピュータに送信する送信手段と、
- 25      を有するコンピュータ・システム。

36. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムとを受信する受信手段と、

- 5 受信された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成する手段と、  
少なくとも前記逆変換データから第1ハッシュ値を計算する計算手段と、  
受信された前記電子署名から第2ハッシュ値を復元する復元手段と、  
計算された前記第1ハッシュ値と復元された前記第2ハッシュ値とを比較し  
10 て改竄の有無を判断する判断手段と、  
を有するコンピュータ・システム。

37. 前記受信手段が、前記フォーマット逆変換プログラムに対する第2の電子署名を受信し、

- 15 前記計算手段が、前記プログラム逆変換プログラムから第3ハッシュ値を計算し、  
前記復元手段が、前記第2の電子署名から第4ハッシュ値を復元し、  
前記判断手段が、計算された前記第3ハッシュ値と復元された前記第4ハッシュ値とを比較して改竄の有無を判断する、  
20 ことを特徴とする請求項36記載のコンピュータ・システム。

38. 送信先向けにフォーマット変換されたデータと少なくともフォーマット変換前のデータに対する電子署名と当該フォーマット変換の逆変換を行うためのフォーマット逆変換プログラムを識別するための識別情報とを受信する受信手段と、

- 25 受信された前記フォーマット逆変換プログラムを識別するための識別情報を用いて、記憶装置から当該フォーマット逆変換プログラムを抽出する手段と、  
抽出された前記フォーマット逆変換プログラムを用いて前記フォーマット変換されたデータを逆変換し、逆変換データを生成する手段と、

前記逆変換データから第 1 ハッシュ値を計算する手段と、  
受信された前記電子署名から第 2 ハッシュ値を復元する手段と、  
計算された前記第 1 ハッシュ値と復元された前記第 2 ハッシュ値とを比較し  
て改竄の有無を判断する手段と、

5      を有するコンピュータ・システム。

1 / 1 0

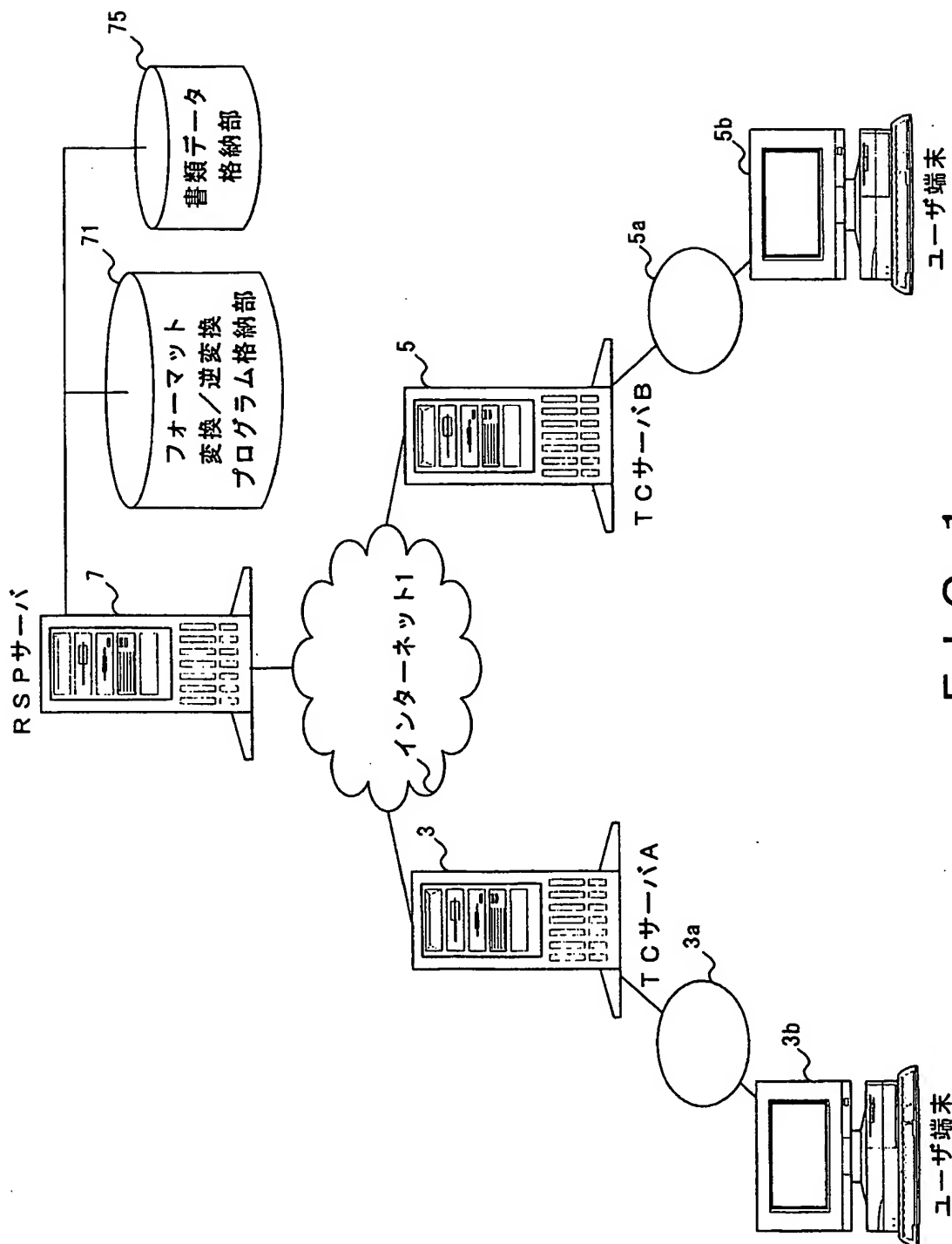


FIG. 1

2 / 1 0

送信先国名	フォーマット 変換プログラム	フォーマット 逆変換プログラム
アメリカ	USA.exe	USA_iv.exe
日本	JPN.exe	JPN_iv.exe
イギリス	UK.exe	UK_iv.exe

F I G . 2

フォーマット 逆変換プログラムID	フォーマット 逆変換プログラム名
USA	USA_iv.exe
JPN	JPN_iv.exe
UK	UK_iv.exe

F I G . 9

3 / 1 0

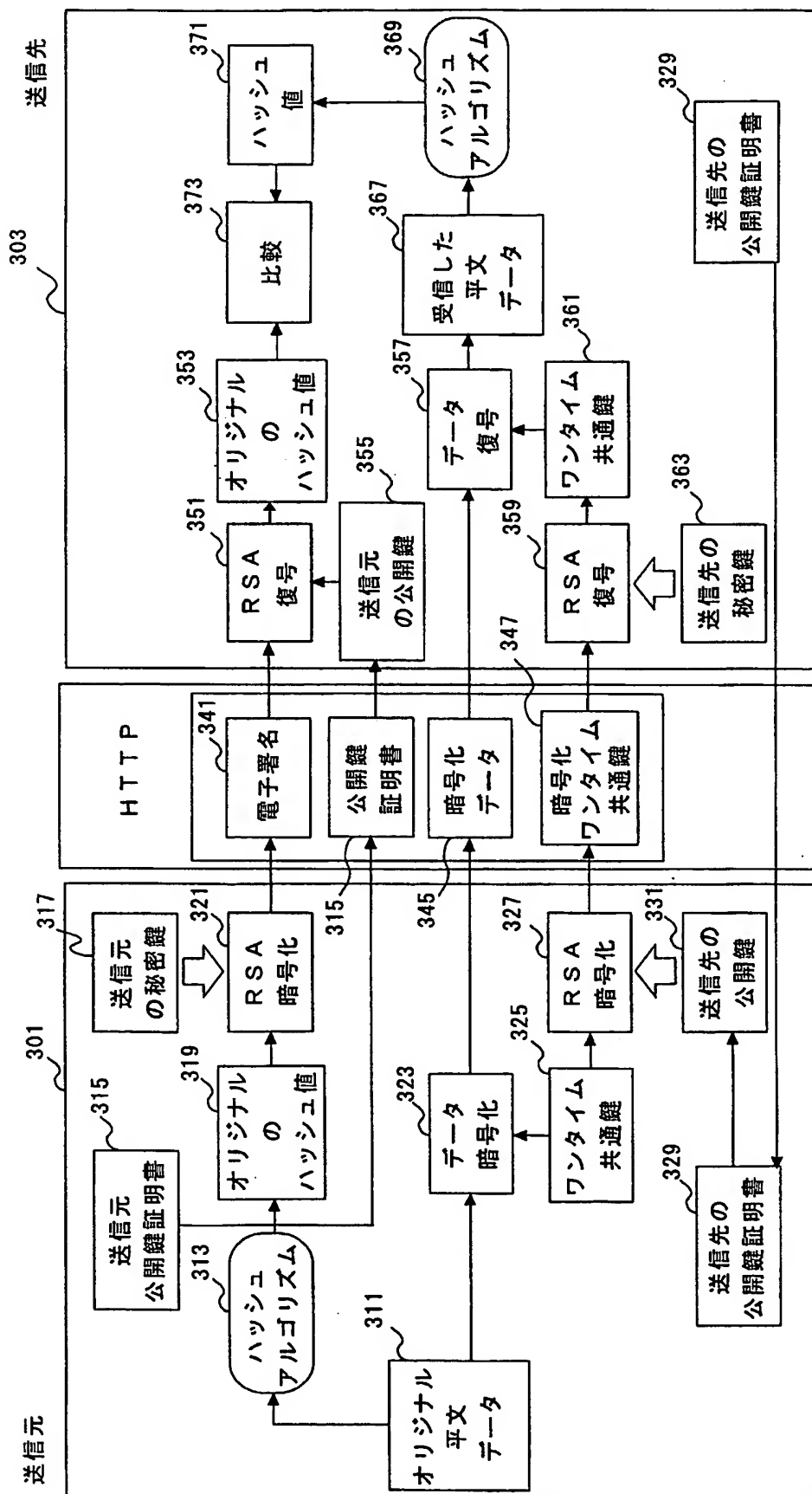
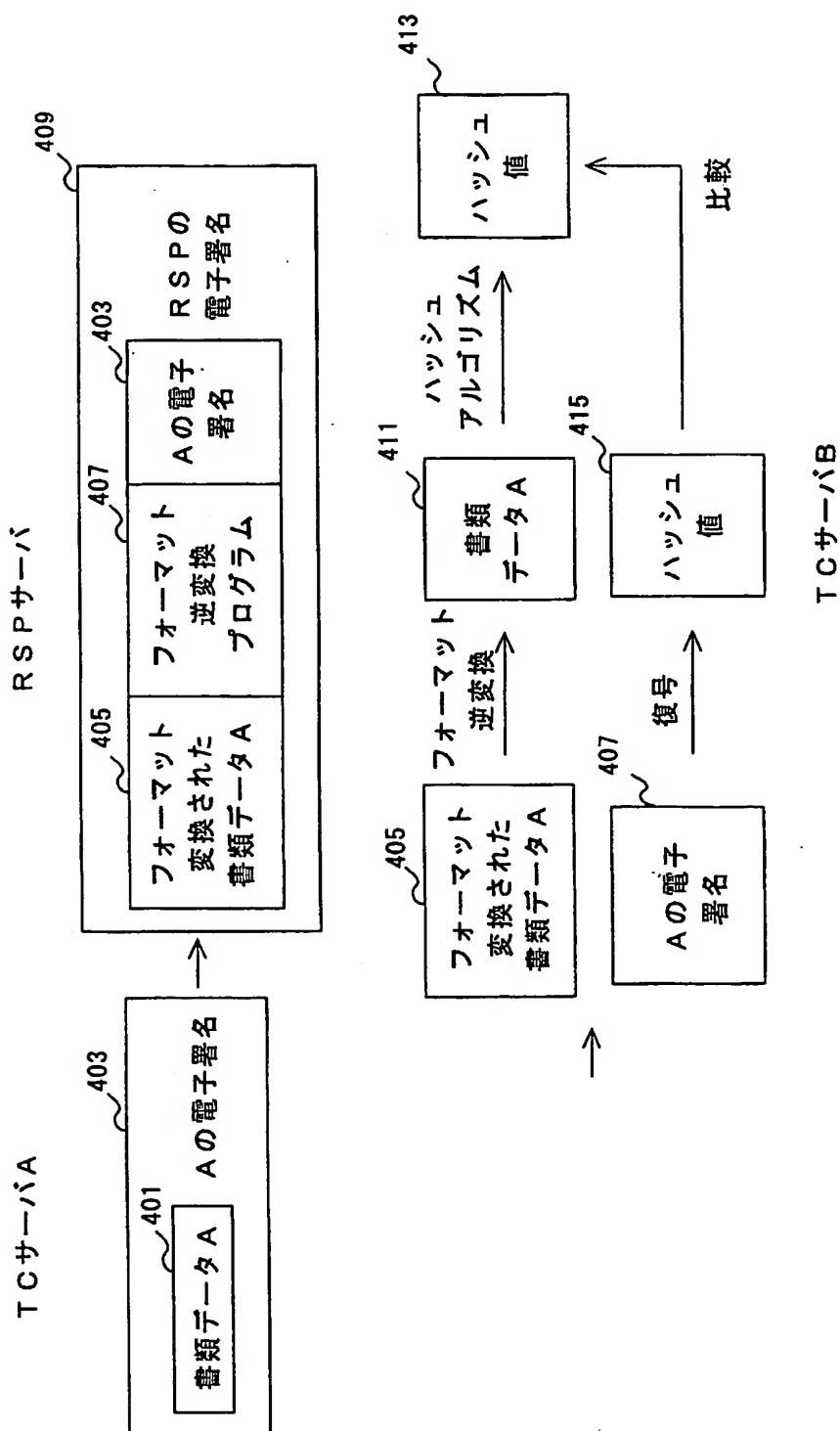


FIG. 3



# Fig. 4

5 / 1 0

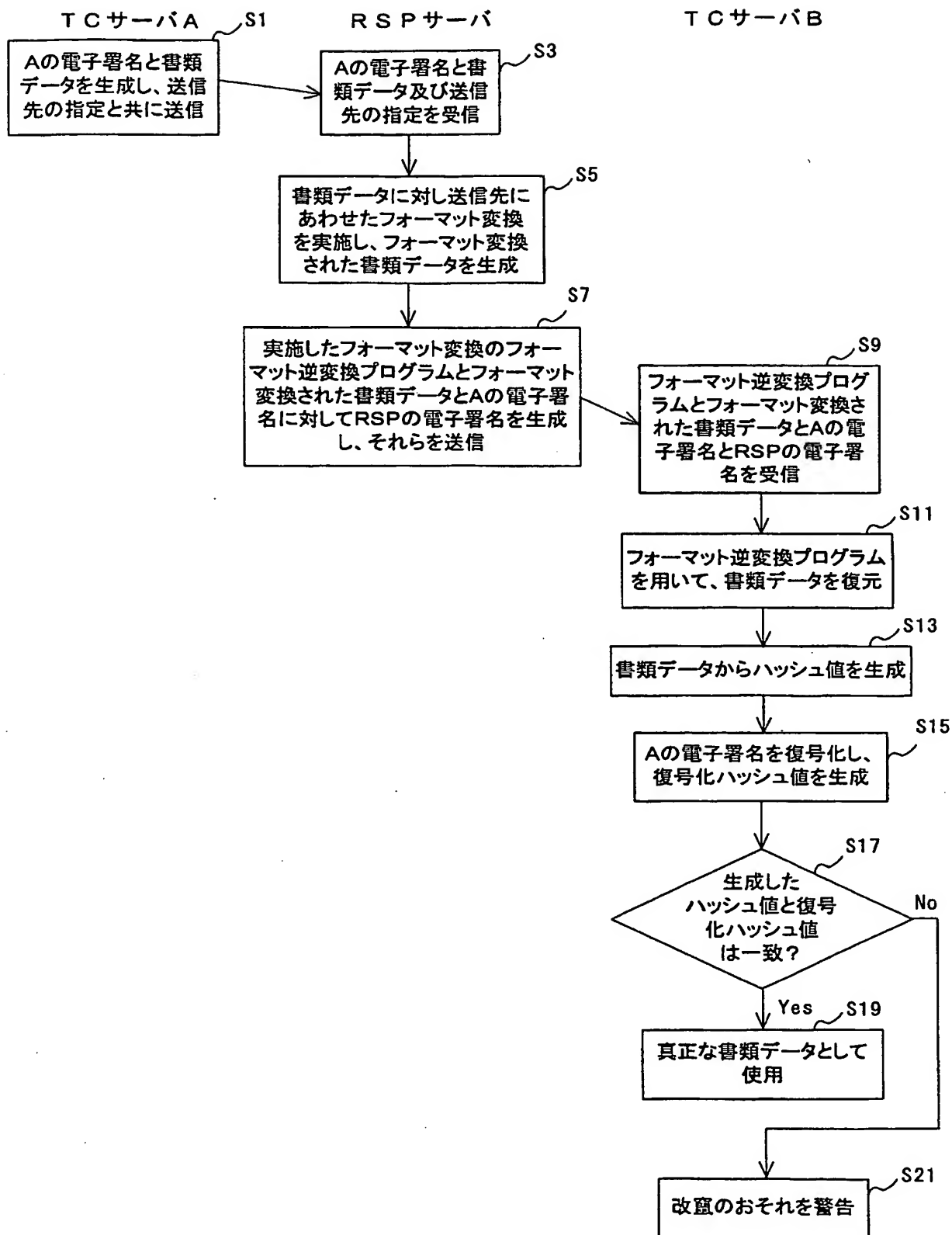


FIG. 5



6 / 1 0

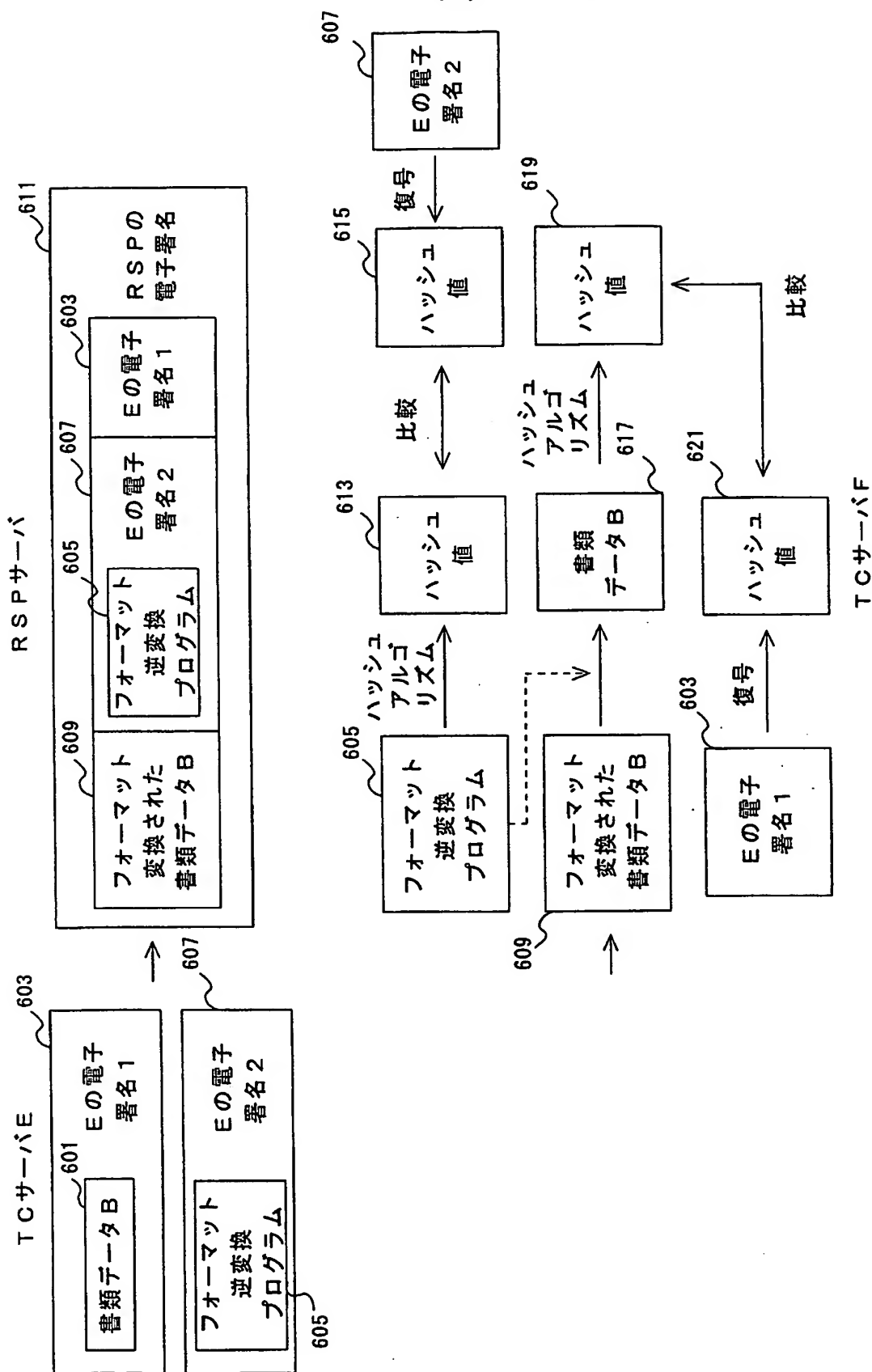


FIG. 6

7 / 10

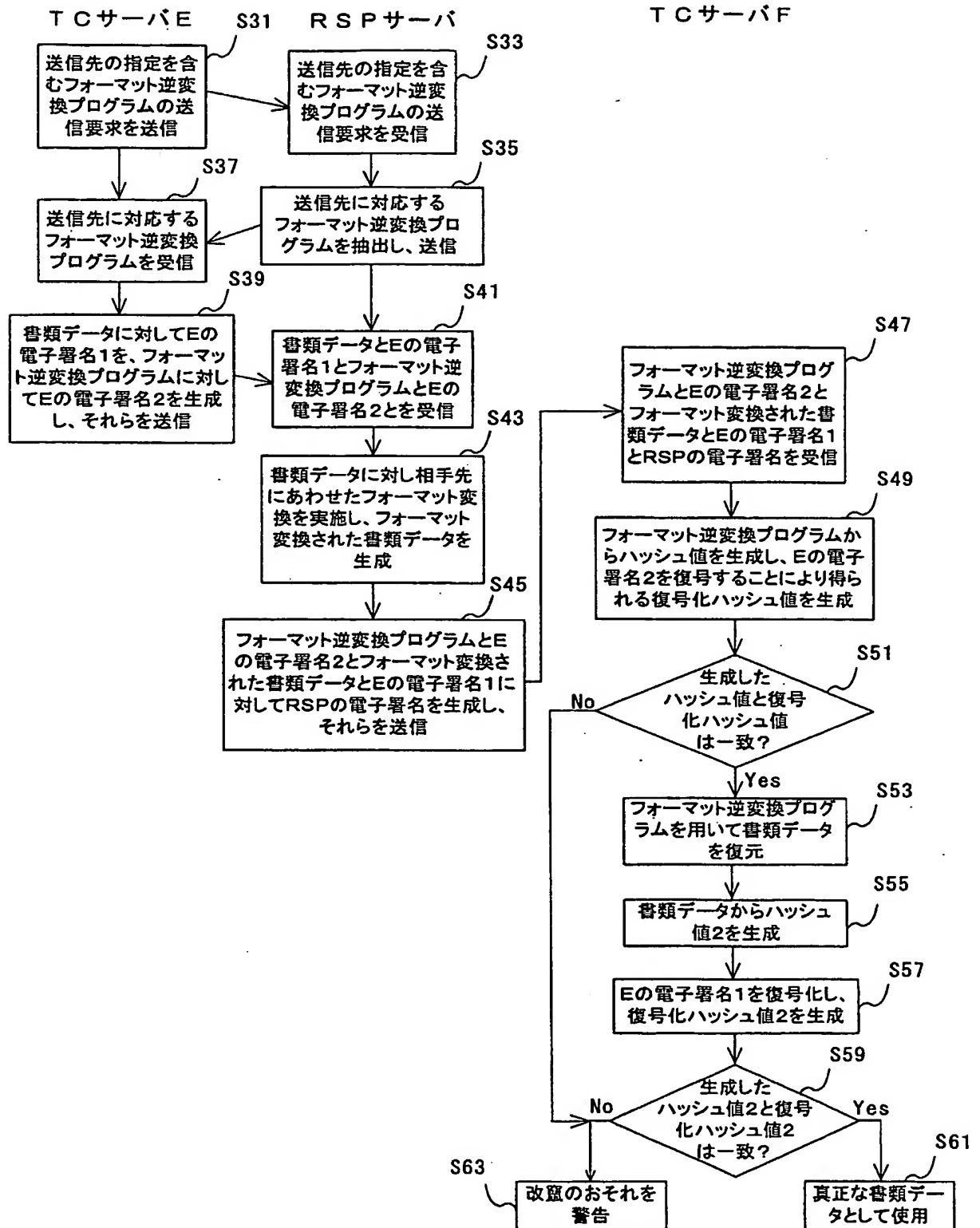


FIG. 7

8 / 10

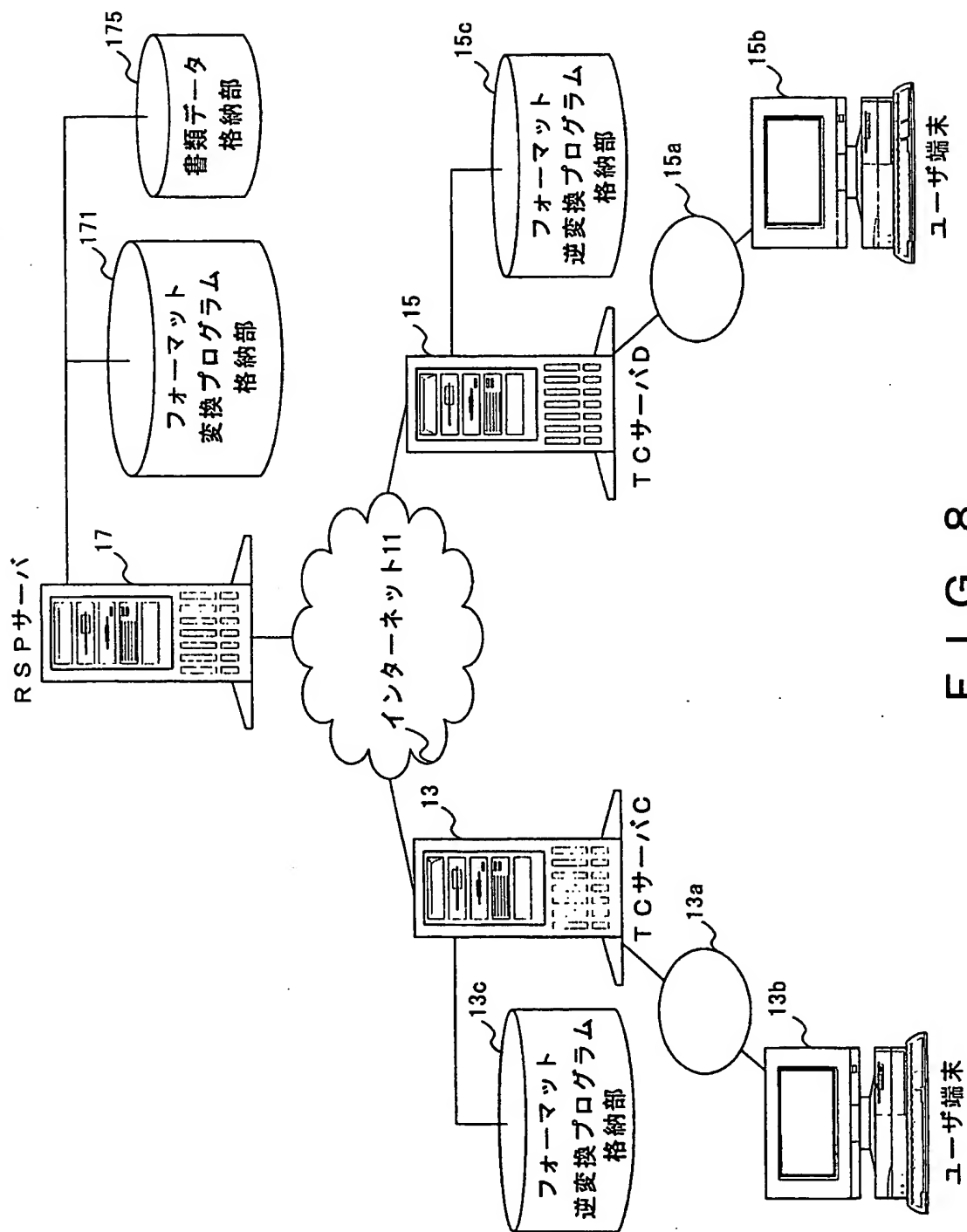


FIG. 8

9 / 10

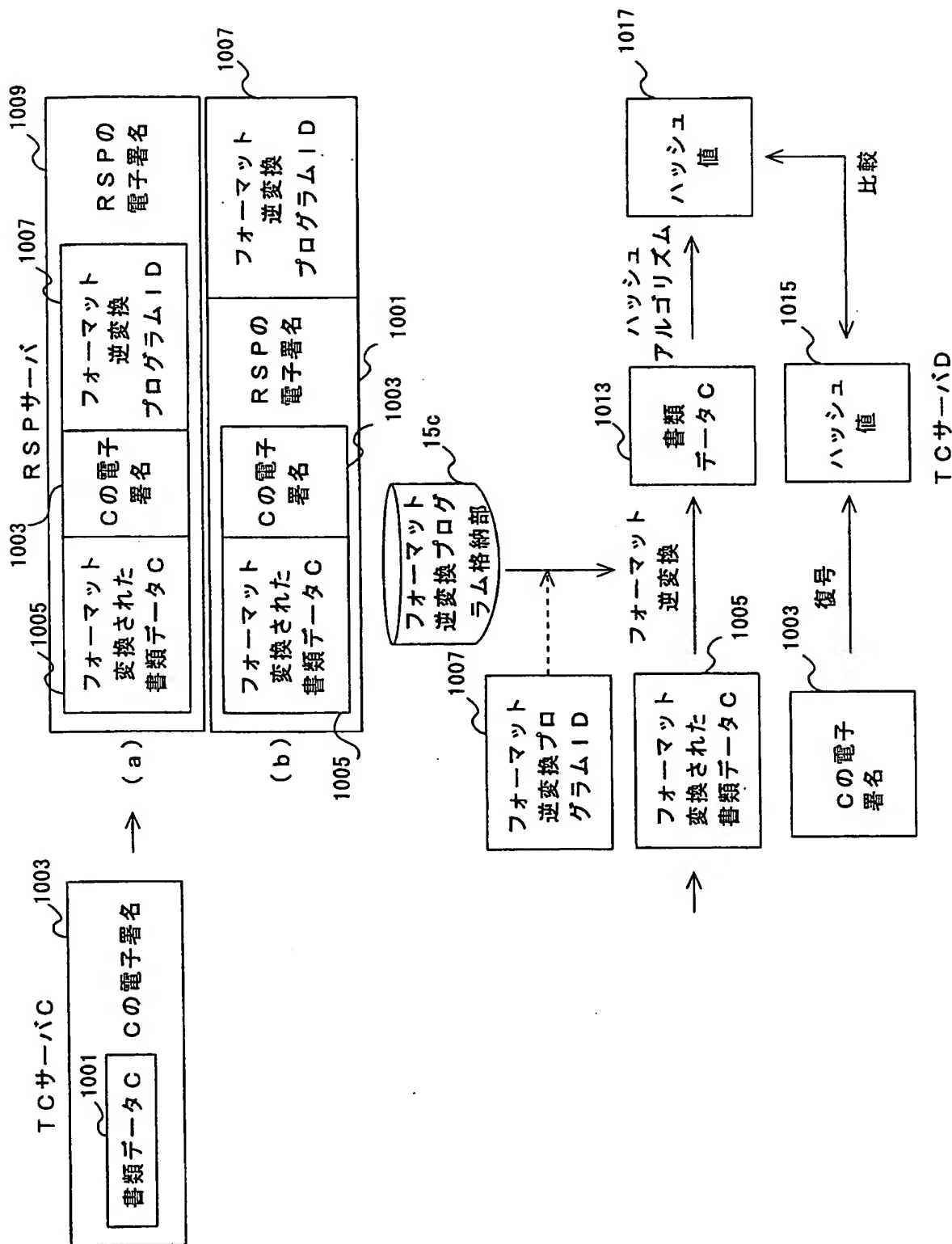


FIG. 10

10 / 10

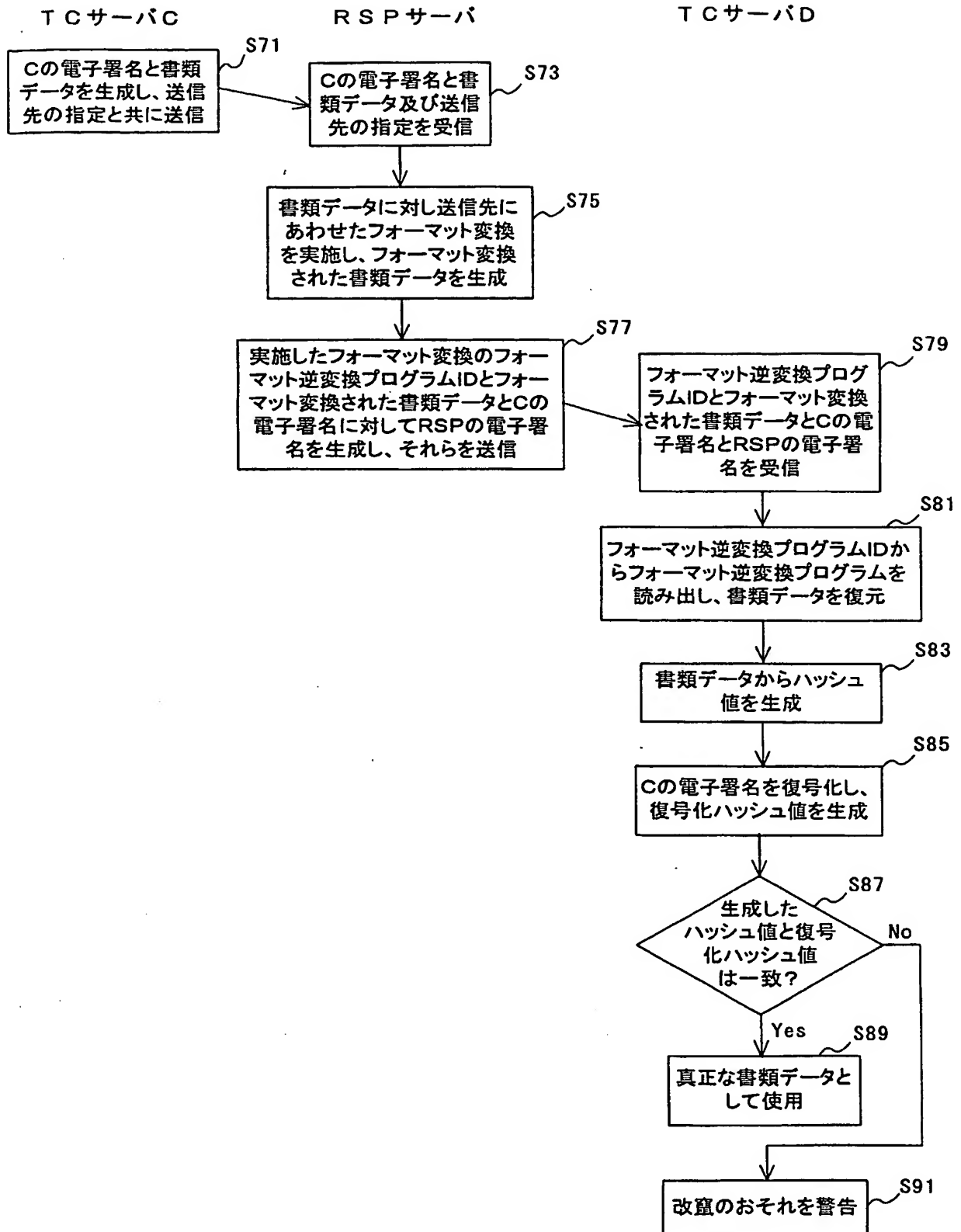


FIG. 11

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05525

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2001  
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-247949 A (Nippon Telegraph and Telephone Corporation), 14 September, 1998 (14.09.1998), page 3, column 3, lines 26 to 32; page 5, column 7, lines 25 to 42; page 5, column 8, lines 27 to 48; page 5, column 8, lines 42 to 48; Figs. 1 to 12 (Family: none)	1-18, 29-38
Y	JP 2000-33868 A (NTT Data Corporation), 08 December, 2000 (08.12.2000), page 4, column 5, lines 2 to 37; page 4, column 6, line 39 to page 5, column 7, line 28; page 7, column 12, line 11 to page 8, column 14, line 21; Figs. 1 to 8 (Family: none)	1-18, 29-38
Y	JP 2000-232442 A (NTT Data Corporation), 22 August, 2000 (22.08.2000), page 3, column 4, lines 37 to 43; page 4, column 5, lines 7 to 30; Figs. 1 to 5 (Family: none)	1-18, 29-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
10 August, 2001 (10.08.01)

Date of mailing of the international search report  
21 August, 2001 (21.08.01)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05525

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-69830 A (Hitachi, Ltd.), 11 March, 1997 (11.03.1997), Full text; Figs. 1 to 18 & US 5966448 A	1-18, 29-38

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05525

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 19-28  
because they relate to subject matter not required to be searched by this Authority, namely:  

A computer program itself is merely a computer language, and a hardware resource functioning by use of the program must solve the problem. The technical matter of the inventions of claims 19-28 is not the one in which information processing by software such as a program is specifically carried out by using hardware resource. Therefore it is not an invention.
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G09C1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年  
 日本国公開実用新案公報 1971-2001年  
 日本国登録実用新案公報 1994-2001年  
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-247949 A (日本電信電話株式会社) 14. 9月. 1998 (14. 09. 98) 第3頁第3欄第26-32行、第5頁第7欄第25-42行、 第5頁第8欄第27-48行、第5頁第8欄第42-48行、 図1-12 (ファミリーなし)	1-18, 29-38
Y	JP 2000-338868 A (株式会社エヌ・ティ・ティ・ データ) 8. 12月. 2000 (08. 12. 00) 第4頁第5欄第2-37行、 第4頁第6欄第39行-第5頁第7欄第28行、	1-18, 29-38

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

10. 08. 01

国際調査報告の発送日

21.08.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M 4229

電話番号 03-3581-1101 内線 3597

## C (続き). 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	第7頁第12欄第11行—第8頁第14欄第21行、図1—8 (ファミリーなし)	
Y	JP 2000-232442 A (株式会社エヌ・ティ・ティ・ データ) 22. 8月. 2000 (22. 08. 00) 第3頁第4欄第37—43行、第4頁第5欄第7—30行、 図1—5 (ファミリーなし)	1-18, 29-38
A	JP 9-69830 A (株式会社日立製作所) 11. 3月. 1997 (11. 03. 97) 全文、図1—18 & US 5966448 A	1-18, 29-38

法第8条第3項（PCT 17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲 19-28 は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
- プログラム自体は単なるコンピュータ言語でしかなく、課題の解決は当該プログラムを用いて機能するハードウェア資源が担うはずであるが、請求の範囲19-28に記載されているものはプログラム等のソフトウェアによる情報処理がハードウェア資源を用いて具体的に実現されたものではないので「発明」には該当しない。
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

次に述べるようにこの国際出願に二以上の発明があるとの国際調査機関は認めた。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

From the INTERNATIONAL BUREAU

**PCT**NOTICE INFORMING THE APPLICANT OF THE  
COMMUNICATION OF THE INTERNATIONAL  
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:

HARADA, Kazuo  
Nishizawa Bldg. 5th Floor  
18-8, Minamisaikai 2-chome, Nishi-ku  
Yokohama-shi, Kanagawa 220-0005  
JAPON

Date of mailing(day/month/year) 09 January 2003 (09.01.03)		<b>IMPORTANT NOTICE</b>	
Applicant's or agent's file reference 0151268			
International application No. PCT/JP01/005525	International filing date(day/month/year) 27 June 2001 (27.06.01)	Priority date(day/month/year)	
Applicant FUJITSU LIMITED, et al			

1. Notice is hereby given that the International Bureau has **communicated**, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this notice:

KR, US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

AU, CA, CN, EP, ID, JP, MX, SG, VN

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this notice is a copy of the international application as published by the International Bureau on 09 January 2003 (09.01.03) under No. WO 03/003329.

4. **TIME LIMITS** for filing a demand for international preliminary examination and for entry into the national phase

The applicable time limit for entering the national phase will, **subject to what is said in the following paragraph**, be **30 MONTHS** from the priority date, not only in respect of any elected Office if a demand for international preliminary examination is filed before the expiration of **19 months** from the priority date, but also in respect of any designated Office, in the absence of filing of such demand, where Article 22(1) as modified with effect from 1 April 2002 applies in respect of that designated Office. For further details, see *PCT Gazette* No. 44/2001 of 1 November 2001, pages 19926, 19932 and 19934, as well as the *PCT Newsletter*, October and November 2001 and February 2002 issues.

In practice, **time limits other than the 30-month time limit** will continue to apply, for various periods of time, in respect of certain designated or elected Offices. For **regular updates on the applicable time limits** (20, 21, 30 or 31 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at <http://www.wipo.int/pct/en/index.html>.

For filing a **demand for international preliminary examination**, see the *PCT Applicant's Guide*, Volume I/A, Chapter IX. Only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination (at present, all PCT Contracting States are bound by Chapter II).

It is the applicant's **sole responsibility** to monitor all these time limits.

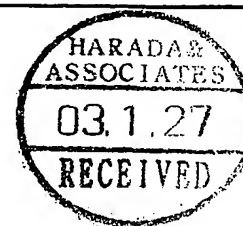
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer  Judith Zahra
Facsimile No.(41-22) 740.14.35	Telephone No.(41-22) 338.91.11

From the INTERNATIONAL BUREAU

**PCT**INFORMATION CONCERNING ELECTED  
OFFICES NOTIFIED OF THEIR ELECTION

(PCT Rule 61.3)

To:

HARADA, Kazuo  
Nishizawa Bldg. 5th Floor  
18-8, Minamisaikai 2-chome, Nishi-ku  
Yokohama-shi, Kanagawa 220-0005  
JAPON

Date of mailing( <i>day/month/year</i> ) 09 January 2003 (09.01.03)		
Applicant's or agent's file reference 0151268		IMPORTANT INFORMATION
International application No. PCT/JP01/005525	International filing date( <i>day/month/year</i> ) 27 June 2001 (27.06.01)	
Priority date( <i>day/month/year</i> )		
Applicant FUJITSU LIMITED, et al		

1. The applicant is hereby informed that the International Bureau has, according to Article 31(7), notified each of the following Offices of its election:  
**EP:** AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR  
**National:** AU, CA, CN, JP, KR, US
2. The following Offices have waived the requirement for the notification of their election; the notification will be sent to them by the International Bureau only upon their request:  
**National:** ID, MX, SG, VN
3. The applicant is reminded that he must enter the "national phase" **before the expiration of 30 months from the priority date before each of the Offices listed above.** This must be done by paying the national fee(s) and furnishing, if prescribed, a translation of the international application (Article 39(1) (a)), as well as, where applicable, by furnishing a translation of any annexes of the international preliminary examination report (Article 36(3) (b) and Rule 74.1).  
  
Some offices have fixed time limits expiring later than the above-mentioned time limit. For detailed information about the applicable time limits and acts to be performed upon entry into the national phase before a particular Office, see Volume II of the PCT Applicant's Guide.  
  
The entry into European regional phase is postponed until **31 months from the priority date** for all States designated for the purposes of obtaining a European patent.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer  Judith Zahra
Facsimile No.(41-22) 740.14.35	Telephone No.(41-22) 338.91.11

## PATENT COOPERATION TREATY

**PCT**  
**NOTIFICATION OF TRANSMITTAL**  
**OF COPIES OF TRANSLATION**  
**OF THE INTERNATIONAL PRELIMINARY**  
**EXAMINATION REPORT**

(PCT Rule 72.2)

From the INTERNATIONAL BUREAU

To:

HARADA, Kazuo  
 Nishizawa Bldg. 5th Floor  
 18-8, Minamisaiwai 2-chome, Nishi-  
 ku  
 Yokohama-shi, Kanagawa 220-0005  
 Japan

<b>Date of mailing (day/month/year)</b> 07 March 2003 (07.03.03)	<b>IMPORTANT NOTIFICATION</b>
<b>Applicant's or agent's file reference</b> 0151268	
<b>International application No.</b> PCT/JP01/05525	<b>International filing date (day/month/year)</b> 27 June 2001 (27.06.01)
<b>Applicant</b> FUJITSU LIMITED et al	

**1. Transmittal of the translation to the applicant.**

The International Bureau transmits herewith a copy of the English translation made by the International Bureau of the international preliminary examination report established by the International Preliminary Examining Authority.

**2. Transmittal of the copy of the translation to the elected Offices.**

The International Bureau notifies the applicant that copies of that translation have been transmitted to the following elected Offices requiring such translation:

EP,CA,CN,US

The following elected Offices, having waived the requirement for such a transmittal at this time, will receive copies of that translation from the International Bureau only upon their request:

AU,ID,JP,KR,MX,SG,VN

**3. Reminder regarding translation into (one of) the official language(s) of the elected Office(s).**

The applicant is reminded that, where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report.

It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned (Rule 74.1). See Volume II of the PCT Applicant's Guide for further details.

<b>The International Bureau of WIPO</b> 34, chemin des Colombettes 1211 Geneva 20, Switzerland  Facsimile No. (41-22) 338.90.90	<b>Authorized officer</b>  Elliott PERETTI (Fax 338 9090)  Telephone No. (41-22) 338 9906
---	---

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 0151268	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/JP01/05525	International filing date (day/month/year) 27 June 2001 (27.06.01)	Priority date (day/month/year)
International Patent Classification (IPC) or national classification and IPC G09C 1/00		
Applicant FUJITSU LIMITED		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p>	
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input checked="" type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>	

Date of submission of the demand 19 October 2001 (19.10.01)	Date of completion of this report 04 April 2002 (04.04.2002)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP01/05525

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☒ the international application as originally filed
- ☐ the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the drawings:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

## 2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

## 3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.



## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP01/05525

## III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 19-28

because:

☒ the said international application, or the said claims Nos. 19-28  
relate to the following subject matter which does not require an international preliminary examination (*specify*):

The subject matters of claims 19-28 are programs to be executed by computers, and do not use any hardware resource during the execution. Therefore, since they merely describe an idea expressing a program source, they relate to a mere presentation of information, which does not require an international preliminary examination by the International Preliminary Examining Authority in accordance with PCT Article 34(4)(a)(i) and Rule 67.1(v).

☐ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. \_\_\_\_\_  
are so unclear that no meaningful opinion could be formed (*specify*):

☐ the claims, or said claims Nos. \_\_\_\_\_ are so inadequately supported  
by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. \_\_\_\_\_.

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Claims	1-18, 29-38	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-18, 29-38	NO
Industrial applicability (IA)	Claims	1-18, 29-38	YES
	Claims		NO

**2. Citations and explanations**

**Claims 1-12 and 29-35**

Document 1: JP, 10-247949, A (Nippon Telegraph and Telephone Corp.), 14 September, 1998 (14.09.98), page 3, column 3, lines 26-32, page 5, column 7, lines 25-42, page 5, column 8, lines 27-48, page 5, column 8, lines 42-48, Figs. 1-12

describes an information processing method, in which (1) an electronic mail and the signature of the sender for the said electronic mail are received from a computer terminal, (2) in the case where the signature has been successfully authenticated, the said electronic mail is converted in a medium that is suitable for the receiver, (3) facsimile image data containing a sending address is produced, and (4) the said facsimile image data is transmitted.

Document 2: JP, 2000-338868, A (NTT Data Corp.), 8 December, 2000 (08.12.00), page 4, column 5, lines 2-37, page 4, column 6, line 39 to page 5, column 7, line 28, page 7, column 12, line 11 to page 8, column 14, line 21, Figs. 1-8

describes a technique, in which signature data is produced for use as a signature covering the basic information converted into another format, to allow authentication also after conversion into the other format.

Document 3: JP, 2000-232442, A (NTT Data Corp.), 22 August, 2000 (22.08.00), page 3, column 4, lines 37-43, page 4, column 5, lines 7-30, Figs. 1-5

describes a technique, in which an authentication program necessary for signature authentication is also distributed to authentication devices.

It is considered to be obvious for a person skilled in the art, to employ the technique of converting also the format of signature data described in document 2, in the information processing method described in document 1, to allow the signature data to be authenticated also on the receiver side after format conversion, in order to avoid the possible inconvenience caused to a data sender or receiver by a falsified message. It is also considered to be obvious for a person skilled in the art as described in document 3, to distribute the program necessary for signature authentication. Furthermore, it is considered to be obvious for a person skilled in the art, to implement an information processing method as a computer system.

**Claims 13-18 and 36-38**

Document 4: "Introduction to Theory of Cryptography (in Japanese)," (Eiji Okamoto), 25 February, 1993 (25.02.93), Kyoritsu Shuppan K.K., Initial Edition, First Impression, pages 129-131

describes a method of checking an identifier prepared by using a hash function, for authentication, as a technique for confirming the authenticity of a message.

**INTERNATIONAL PRELIMINARY EXAMINATION REPORT**

International application No.

**PCTJP01/05525****Supplemental Box**

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of : V.2

It is considered to be obvious for a person skilled in the art, to employ the technique of converting also the format of signature data described in document 2, in the information processing method described in document 1, to allow the signature data to be authenticated also on the receiver side after format conversion, in order to avoid the possible inconvenience caused to a data sender or receiver by a falsified message. Furthermore, it is a well-known commonly used technique described in document 3, to distribute the program necessary for signature authentication, and it is also a well-known commonly used technique described in document 4, to use a method of checking an identifier prepared by using a hash function, as a method of realizing signature authentication. So, employing these techniques is considered to be obvious to a person skilled in the art. Moreover, it is considered to be obvious for a person skilled in the art, to implement an information processing method as a computer system.